El Software Libre como herramienta del hacktivismo contra el cibercontrol social

Pablo Garaizar Sagarminaga
Universidad de Deusto
garaizar@eside.deusto.es

versión 1.0

1 de noviembre de 2004

'Sed quis custodiet ipsos custodes.'

Juvenal (ca. 60 to 130 AD), Sat. 6, 347

Resumen

La información es el principal recurso de poder de nuestros días. Sin embargo, su flujo continuo y saturado devalúa gran parte de esa información, y se hace necesario procesarla automáticamente para filtrarla y asimilarla. Gobiernos y empresas entendieron esto rápidamente hace tiempo y emplean masivamente la Red para extraer conocimiento acerca de todo lo que les pueda interesar. Una persona, un consumidor, repiten las empresas. Una persona, un posible enemigo, replican los gobiernos.

Como reacción a este continuo escrutinio que pone en peligro nuestra intimidad surge la figura del hacktivista, una suma de activista y apasionado de la tecnología (hacker). El hacktivista conoce la Red y el software que la gestiona. Se ha hecho un experto gracias a las posibilidades que le ha brindado el Software Libre, y ha creado multitud de herramientas para detener esa invasión a su privacidad.

En el presente texto veremos en qué consiste el Software Libre, cuáles son esas medidas de control social telemático y qué alternativas propone el movimiento hacktivista, haciendo hincapié en su capacidad de modificación de las nuevas tecnologías en beneficio del cambio social.

¿Qué es el Software Libre?

La informática no dejó de ser un conjunto de calculadoras gigantes, carísimas y difíciles de manejar hasta que Thompson y Ritchie, de los laboratorios Bell, desarrollaron el sistema UNIX a comienzos de los años 70. Con este sistema se rompió la incompatibilidad que reinaba entre los diferentes ordenadores de la época. En lugar de

usar métodos propios de cada fabricante, se basaron en estándares y formatos abiertos para su desarrollo. Lograron un "esperanto" entre las máquinas. Sin embargo, la portabilidad requería de un esfuerzo. Las universidades y laboratorios se comunicaban entre sí para poder portar código a una máquina en concreto, o para compartir un driver [1] de una impresora, por ejemplo. Muchas personas casi anónimas fueron aportando su pequeño granito de arena a este Sistema Operativo[2]. La informática era algo artesanal, se compartía el código de la misma manera que la gente comparte recetas de cocina. Nadie hablaba de "Software Libre" por aquel entonces, era lo habitual (nadie llama "Gastronomía Libre" al hecho de que mi madre le dé la receta del pastel de manzana a su prima).

Sin embargo, fue en esta época cuando el modelo de negocio de comercialización del software tuvo su arranque. Cada vez más empresas fueron haciendo privado o cerrado su código, obligando a firmar acuerdos de "no divulgación" ("non-disclosure") a quienes adquirieran ese software[3]. El fabuloso recetario de cocina que se había ido formando con las aportaciones de tanta gente se hizo privado. Las nuevas "recetas" o programas ya no podrían consultarse más: o comprabas el pastel o no lo comprabas, pero ya no podías ver cómo estaba hecho. La mayoría de los mejores administradores de sistemas de la época fueron reclutados por esas empresas de software, ofreciendo contratos millonarios.

Los "hackers"[4] de los setenta cambiaron su concepción del software ayudados por las generosas sumas de sus nóminas. Por este entonces, Richard Stallman, un hacker experto en Sistemas Operativos de tiempo compartido en el MIT (Instituto Tecnológico de Massachusetts), decide romper con esta dinámica de ocultación y privatización del software y funda la "Free Software Fundation" (FSF). La FSF es un proyecto sin ánimo de lucro que pretende mantener la libertad en el software. Para asegurar esa libertad, renuncia a su sueldo en el MIT y se enfrasca en un proyecto titánico: crear un Sistema Operativo totalmente libre. Lo primero que necesita para ponerse a escribir esta leyenda es lápiz y papel, es decir, en términos informáticos, un editor. Haciéndose valer de sus amplias capacidades como programador, Stallman crea "Emacs", un potente editor que distribuye de forma libre. Gracias al soporte proporcionado y a las copias en cinta que vendía, pudo obtener los ingresos suficientes como para continuar con su proyecto. Además, en el MIT se le permitió utilizar algunos ordenadores de los laboratorios y se le mantuvo su despacho sin pedir nada a cambio.

Stallman había dado un gran paso creando "Emacs", además de proporcionarse una fuente de ingresos, podía generar documentación y código de manera libre. El siguiente paso lógico fue diseñar un compilador para poder crear programas ejecutables de forma libre. Si el código fuente de un programa puede entenderse como la "receta" del pastel, el compilador es el "horno", que transforma la receta en pastel, es decir, el programa fuente en programa ejecutable. Así es como surgió el GCC, Compilador de C GNU. Con él ya se podían crear programas que no dependieran de licencias cerradas. Teníamos toda la tinta y papel que quisiéramos para escribir las recetas (el editor), y hornos gratis para todos; los pasteles no tardarían en llegar. El proyecto de crear un Sistema Operativo totalmente libre tomó el nombre de GNU. GNU es un acrónimo recursivo que significa "GNU's Not UNIX", es decir, "GNU no es UNIX". El Sistema Operativo de la FSF sería compatible con UNIX, pero no sería un UNIX comercial.

Gracias a esta compatibilidad con UNIX, el proyecto GNU se pudo enfocar de manera modular: partiendo de un UNIX comercial, se fueron desarrollando y sustituyendo cada una de sus partes propietarias por sus equivalentes libres, poco a poco. Imaginémonos a GNU como un gran Frankstein, que vamos componiendo con las partes del cuerpo que vamos produciendo. Dentro de la comunidad del Software Libre había gente que era capaz de hacer desarrollos muy importantes, siguiendo con el símil producirían partes importantes del cuerpo, como el corazón, los pulmones, etc. Los programadores no tan buenos contribuían a su vez haciendo aportaciones pequeñas pero útiles. Diseñaban las uñas de nuestro Frankstein, los pulgares, cosas sencillas.

Stallman había dado un gran paso creando "Emacs", además de proporcionarse una fuente de ingresos, podía generar documentación y código de manera libre. El siguiente paso lógico fue diseñar un compilador para poder crear programas ejecutables de forma libre. Si el código fuente de un programa puede entenderse como la "receta" del pastel, el compilador es el "horno", que transforma la receta en pastel, es decir, el programa fuente en programa ejecutable. Así es como surgió el GCC, Compilador de C GNU. Con él ya se podían crear programas que no dependieran de licencias cerradas. Teníamos toda la tinta y papel que quisiéramos para escribir las recetas (el editor), y hornos gratis para todos; los pasteles no tardarían en llegar.

El proyecto de crear un Sistema Operativo totalmente libre tomó el nombre de GNU. GNU es un acrónimo recursivo que significa "GNU's Not UNIX", es decir, "GNU no es UNIX". El Sistema Operativo de la FSF sería compatible con UNIX, pero no sería un UNIX comercial. Gracias a esta compatibilidad con UNIX, el proyecto GNU se pudo enfocar de manera modular: partiendo de un UNIX comercial, se fueron desarrollando y sustituyendo cada una de sus partes propietarias por sus equivalentes libres, poco a poco. Imaginémonos a GNU como un gran Frankstein, que vamos componiendo con las partes del cuerpo que vamos produciendo. Dentro de la comunidad del Software Libre había gente que era capaz de hacer desarrollos muy importantes, siguiendo con el símil producirían partes importantes del cuerpo, como el corazón, los pulmones, etc. Los programadores no tan buenos contribuían a su vez haciendo aportaciones pequeñas pero útiles. Diseñaban las uñas de nuestro Frankstein, los pulgares, cosas sencillas.

A finales de los ochenta el proyecto GNU estaba casi terminado, pero carecía de un kernel o núcleo del sistema bien desarrollado: Frankstein tenía un cuerpo perfectamente acabado, pero le faltaba el cerebro. Casualmente por esas fechas, un joven estudiante de la Universidad de Helsinki comenzó un proyecto personal, sólo para divertirse ("just for fun!"): Linux. Lo maravilloso de Linux ha sido que, ayudándose de Internet, ha movilizado a un montón de gente que fue desarrollándolo en paralelo, de forma no jerarquizada, casi caótica.

El resultado era espectacular, los nuevos diseños y mejoras se sucedían semana tras semana. ¡El modelo "bazar" de desarrollo estaba dando mejores frutos que el modelo "catedral"![5] Como ya hemos dicho, Linus Torvalds se ayudó de Internet para explicar su proyecto y solicitar ideas y colaboraciones. Pronto la Red se volcó en el desarrollo de ese núcleo, y en pocos meses se obtuvieron versiones operativas. Inicialmente ese núcleo iba a llamarse FreaX, en alusión a su carácter libre, y haciendo un juego de palabras entre la voz inglesa "free" (libre), "freak" (extraño, raro) y la X final de todos

los UNIX. Ari Lemke, un compañero suyo, no estaba nada convencido de ese nombre, y decidió cambiarlo a LinuX, una mezcla de Linus y UNIX.

Si Linux es sólo el núcleo del Sistema Operativo, ¿por qué tanta gente llama "Linux" a todo el Sistema Operativo? Bien, realmente el conjunto del núcleo más el resto de aplicaciones que conforman todo el Sistema Operativo se llama "GNU/Linux". De la misma manera que muy poca gente llama "horno microondas" a su microondas, muy pocos llaman "GNU/Linux" a su sistema Linux. Este hecho suele fastidiar a los partidarios de GNU, si bien es cierto que no todo lo que se conoce como "GNU/Linux" proviene de la suma de "GNU" + "Linux", ya que existe mucho software diferente dentro del sistema. Linus Torvalds, aquel estudiante que inició el desarrollo de Linux, decidió distribuir Linux bajo la licencia GPL de la Free Software Fundation. Esta licencia asegura que tanto Linux como todas sus variaciones permanecerán siendo Software Libre, es decir manteniendo las cuatro libertades del software:

1. La libertad de usar el programa, con cualquier propósito (Libertad 0).
2. La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades (Libertad 1).
3. El acceso al código fuente es una condición previa para esto. La libertad de distribuir copias, con lo que puedes ayudar a tu vecino (Libertad 2).
4. La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. (Libertad 3). El acceso al código fuente es un requisito previo para esto.

Gracias a esta decisión, Linux era un núcleo de Sistema Operativo libre, y GNU era un Sistema Operativo libre a falta de núcleo, por lo que el matrimonio GNU/Linux resultó algo casi obvio. Por primera vez desde la privatización del mundo del software, podíamos utilizar un Sistema Operativo totalmente libre. El binomio GNU/Linux es el más conocido de los productos de la comunidad del Software Libre, pero no el más exitoso. A pesar de que GNU/Linux multiplica cada pocos meses su número de usuarios, todavía no ha llegado a tener una cuota de usuarios realmente significativa con los sistemas y programas y sabe cómo sacarles el máximo provecho, al contrario que la mayoría de los usuarios que prefieren conocer sólo lo imprescindible. Todo lo contrario sucede en el campo de los Servidores Web: Apache, con más del 60% de cuota[6], es el servidor más usado con diferencia, a mucha distancia de su más inmediato competidor. Apache es el ejemplo paradigmático de la plausibilidad del Software Libre como software profesional, bien acabado y diseñado, utilizable en entornos de producción reales con unos resultados altamente satisfactorios. No se puede decir lo mismo del Internet Information Server, de Microsoft, a pesar de las diferencias en cuanto a presupuesto.

Como vemos, el mundo del software tiene implicaciones sociales grandes. que no deberían ser obviadas a la hora de adquirir nuestros programas. Hablamos de "free software", pero "libre como en "libertad de expresión", no como en "barra libre"[7]". Es decir, poniendo el énfasis en la libertad del software, no en su gratuidad. Más adelante analizaremos las posibilidades del software libre como herramienta de cambio social y

lucha telemática por parte de activistas de la Red.

El cibercontrol social

Bajo este angustiante nombre se enmarcan las diferentes técnicas que se han venido desarrollando en el último cuarto de siglo para controlar al ciudadano de a pie tanto dentro de las redes de comunicación globales como fuera de ellas. Olvidemos las películas de serie B de espías y contra-espías en el Telón de Acero, el objetivo ahora es cualquier ciudadano, en principio anónimo, que tenga potencialmente algo que esconder. El progreso tecnológico ha permitido esta labor que hace bien poco se antojaba imposible, aprovechándose además del amparo y la falsa sensación de anonimato que provoca el uso de Internet.

Sistemas de control en Internet

Desde los comienzos de Internet, cuando la antigua Arpanet tenía mucho más de aldea que de global, el proyecto Echelon ya funcionaba interceptando contenidos considerados como peligrosos en las comunicaciones electrónicas. En un principio nadie quiso creer paranoicas historias sobre sistemas de espionaje computerizado, satélites vigilando noche y día nuestras comunicaciones, filtros de correo electrónico, etc. Todo parecía sacado de una vieja película de espías. Sin embargo, 30 años después de su constitución en 1971, el Parlamento Europeo hizo pública su existencia en mayo de 2001:

"(...) No hay ninguna razón para seguir dudando de la existencia de un sistema de intercepción de las comunicaciones a nivel mundial en el que participan los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda en el marco del Acuerdo UK/USA; considerando, asimismo, que según las informaciones de que se dispone, es probable que su nombre sea "ECHELON", si bien no es éste un aspecto de importancia primordial (...) El sistema no se utiliza para interceptar comunicaciones militares, sino privadas y económicas (...)[8]"

Como vemos el sistema está orientado al espionaje del ciudadano de a pie en su vida cotidiana, atrás quedó el espionaje militar de la guerra fría, todo el mundo es un enemigo potencial. No sólo las comunicaciones personales por Internet son filtradas y espiadas, sino muchas conversaciones telefónicas, celulares, fax y GPS. Funciona con un sistema de "palabras clave" que activan el filtrado. Un ejemplo bastante escandaloso de este sistema es el que se relató en el programa "60 minutes" de la CBS. Una mujer hablaba por teléfono con una amiga explicándole que su hijo hizo un papel durante una obra de teatro en el colegio, usando la expresión "he bombed" (literalmente "puso una bomba", pero también en sentido figurado "fue muy deprisa"). El sistema detectó automaticamente la expresión, y su nombre y datos personales fueron a parar a la base de datos de posibles terroristas.

El "mejor" Gran Hermano jamás diseñado ha estado más de un cuarto de siglo espiando conversaciones por todo el mundo. La alianza entre las agencias de seguridad e inteligencia de todos sus participantes se han cubierto las espaldas en el terreno legal: es ilegal que un gobierno espíe a sus propios ciudadanos y mandatarios, pero siempre es posible pedir "favores" al resto de participantes en este sentido. Margaret Tatcher hizo

uso de estos favores y espió a varios miembros de su gabinete solicitando informes a sus colegas canadienses. Organizaciones como Greenpeace o Amnistía Internacional han sido también espiadas, como se ha reconocido públicamente[9].

Obviamente esto sólo es la punta del iceberg, sin embargo cada vez la cantidad de información que hay que tratar se va haciendo más inmanejable y su eficacia está cayendo poco a poco. Por esto mismo, la NSA, Agencia de Seguridad Nacional de Estados Unidos, y el FBI están desarrollando nuevas herramientas para aumentar la capilaridad de sus sistemas de filtrado y espionaje. En este sentido destacan las colaboraciones de empresas que guían gran parte del futuro de Internet como Microsoft [10] o Cisco, líderes en el mercado del software y el hardware de equipamientos de red respectivamente. Ambas empresas han manifestado públicamente que supeditarán la privacidad de sus usuarios a los intereses de la NSA y FBI en cuestiones de seguridad. Este colaboracionismo se ha visto como algo muy negativo dentro de los grupos de usuarios concienciados con el tema, pero la gran mayoría de sus consumidores no se detienen a observar estos puntos de la licencia EULA (End User License Agreement) que aceptamos cada vez que instalamos uno de sus productos.

Además de los acuerdos de colaboración con Microsoft o Cisco entre otros, el FBI ha contado con la colaboración de hackers afamados como el grupo "Cult of the Dead Cow [11]", creador de la famosa herramienta de "administración remota" de sistemas (a veces considerada como software espía o troyanos) "Back Oriffice". Esto le ha hecho trabajar en la creación de programas espía (spyware) como "Magic Lantern[12]" o "Cyber Knight", programas capaces de editar el registro de Microsoft Windows, detectar claves secretas, manipular archivos o espiar conversaciones por chat, Messenger o ICQ.

Carnivore[13] es un proyecto en este mismo sentido. En palabras de los propios representantes del FBI "Carnivore es un sistema computacional diseñado para permitir al FBI; en colaboración con un proveedor de Internet (ISP) se haga valer una orden judicial que exige la recolección de cierta información en relación al correo electrónico u otros tipos de comunicaciones electrónicas de un usuario específico que es objeto de investigación". Como podemos ver, Carnivore solicita la colaboración de los proveedores de Internet, pidiendo los registros de correos electrónicos enviados o recibidos por y para una persona en concreto. Esto es bastante similar a lo que la nueva Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE), que obliga a guardar los registros de todo lo que sucede en proveedores de Internet y demás empresas que desarrollen actividades comerciales en Internet. A pesar de las protestas de asociaciones de internautas y grupos sociales relacionados con la telemática, el gobierno español ha seguido adelante con la ley, cuyo reglamento es a día de hoy una incógnita y podría afectar muy negativamente a las libertades digitales de mucha gente.

Por otro lado, sistemas como Microsoft Passport.Net pueden ser una amenaza grande contra la intimidad de los "netizens" o ciudadanos de la red. Mediante Passport.Net es posible introducir un usuario y contraseña en uno de los sitios en los que se utilice y no tener que volver a enseñar ese "pasaporte virtual" en el resto de sitios que funcionan con este sistema[14]. Es muy habitual que entremos en Hotmail a revisar nuestro correo, vayamos a Amazon.com a comprar un libro o a Ebay a buscar algo en sus subastas y

que esos sitios nos reconozcan al entrar y nos muestren nuestras preferencias, etc. Esto no supondría mayor riesgo si el sistema no pudiera utilizarse para hacer correlaciones complejas que dieran más información que la estrictamente necesaria para cada una de esas tiendas virtuales. Pongamos un ejemplo: si un hombre mediante Passport.Net compra unos pantys en una web de lencería, cualquiera podría pensar que son para su madre, hermana o novia. Si mediante este mismo sistema se hace con el mapa de calles de Leganés, es probable que vaya a pasar una temporada por allí, de vacaciones o por trabajo. Si además de esto, se compra una escopeta de caza, el sitio que se la vende pensará que tiene un coto privado, y si compra una sierra para cortar metales, es probable que quiera hacer obras en las cañerías de casa. El "problema" para este sujeto viene al ver todos estos datos a la vez, junto con la noticia de que un encapuchado ha asaltado una caja de ahorros en Leganés a punta de escopeta recortada.

Sistemas de control en Telefonía móvil

Desde el principio de la telefonía móvil ha sido posible localizar y rastrear geográficamente un teléfono conectado a la red. De hecho, esto es un principio básico en las redes telefónicas móviles, es necesario para poder seguir dando servicio cuando un teléfono se mueve de una posición a otra. Cualquier gobierno u organización con capacidad de controlar las redes de telefonía móvil tiene la posibilidad de averiguar la posición de un teléfono en cada momento, o lo que suele ser lo más habitual, de su propietario.

La parte técnica de este seguimiento continuo del individuo es muy sencilla. Las antenas de telefonía móvil necesitan emitir en todas las direcciones, porque deben funcionar con independencia de en qué dirección se encuentre la persona que quiere usar su teléfono. Sin embargo, en lugar de utilizar antenas que emitan en 360 grados, usan 3 antenas que emiten en sectores de 120 grados, porque son más sencillas de construir. Cuando un teléfono móvil está encendido, intenta conectarse con el mayor número de antenas posible para tener mejor cobertura y no perder la conexión con la red telefónica en ningún momento. Entonces, sabiendo a qué antenas se ha conectado un teléfono móvil en concreto, podemos trazar un polígono en el que con total seguridad se encontrará el teléfono buscado. Es decir, si yo me encuentro en mitad de una plaza y hay torres de telefonía móvil en las cuatro esquinas de la plaza, mi teléfono se habrá conectado a las cuatro torres utilizando las antenas que apuntan hacia él, por lo tanto es muy sencillo deducir que el teléfono se encontrará en el área comprendida entre las cuatro antenas implicadas. La localización de un teléfono móvil empleando este procedimiento tiene una precisión bastante similar a la que podría proporcionar un servicio de GPS de uso civil sin corrección de errores, aunque como se puede intuir, cuanta mayor sea la densidad de antenas en una zona en concreta, mayor será la precisión obtenida.

Actualmente bastantes compañías telefónicas y otras empresas asociadas ofrecen este servicio a costes muy bajos[15], cobrando únicamente el coste del envío de un SMS o mensaje corto a la central de localización. Esto ha aumentado su uso en situaciones en las que el propietario del teléfono móvil ha dado su consentimiento -tácitamente o no- para ser localizado, como por ejemplo en empresas de transportes, o adolescentes con teléfono móvil, por citar dos ejemplos típicos.

Burlar estos sistemas de localización es prácticamente imposible si quien lo intenta

pretende seguir utilizando la red telefónica móvil, puesto que como hemos dicho al principio, es un pilar básico para que esta red funcione correctamente. Sin embargo hay esfuerzos por parte de hackers o phreakers (hackers expertos en telefonía) para introducir retardos aleatorios en su señal con vistas a despistar a sistemas rastreadores e incrementar sus márgenes de error. De todas maneras, estos intentos no son más que una pequeña molestia para el sistema de localización y no lo anulan.

Sistemas de control en la vida cotidiana

Ya no es necesario utilizar Internet o poseer un teléfono móvil para ser rastreado y controlado a diario, el simple hecho de hacer la compra en un supermercado puede convertir nuestra despensa en un localizador a distancia.

A finales de los noventa, un grupo de investigadores del M.I.T. se dio cuenta de que sus esfuerzos para que los sistemas automáticos de reconocimiento de objetos que estaban desarrollando detectaran la realidad en toda su complejidad eran poco provechosos y decidieron ayudar a estas máquinas ideando unas etiquetas de auto-identificación para cada objeto (Auto-ID)[16]. Así, un libro tendría una etiqueta que informara al sistema de reconocimiento de que era un libro, proporcionando además datos sobre su autor, fecha de publicación, editorial, etc., y una botella de agua podría hacer lo propio, indicando además su fecha de embotellado y su fecha de caducidad. Esta mejora en los sistemas de reconocimiento pronto se vio como una oportunidad para la gestión de stocks, sobre todo en el campo de la alimentación y las grandes superficies comerciales.

La cadena estadounidense Wal-Mart está decidida a obligar en 2006 a sus 100 mayores proveedores a sustituir la identificación de sus productos mediante código de barras por esta nueva tecnología, que tiene el nombre de RFID (Radio-Frequency IDentification). De esta manera se solucionarán sus problemas para tener consciencia del estado exacto de sus estanterías en cada momento. Bastará emitir una leve señal de radio para que los pequeños circuitos RFID adheridos a cada producto se carguen eléctricamente y emitan su posición exacta. El sueño de cualquier encargado de stocks ya está aquí.

El chip RFID tiene el aspecto de un chip empleado para evitar robos: consta de una espiral metálica más o menos amplia que sirve como antena y un pequeño chip que es el que contiene la información. En los RFID pasivos no es necesario alimentar el circuito con baterías, basta emitir una señal de radio adecuada para que el circuito se cargue al recibirla y sea capaz posteriormente de emitir una señal de vuelta. Funcionarían en ese caso como una clase de "reflectores", reflejando la señal recibida, parcialmente modificada. Esto hace que cualquier objeto sea susceptible de portar un chip RFID de forma bastante inocua para quien lo posee.

En este mismo sentido, bibliotecas estadounidenses como la Berkeley Public Library han optado a su vez por esta tecnología para llevar un registro del préstamo de libros[17]. Cada libro tiene adherido un chip RFID que lo identifica unívocamente y permite contabilizar cuántos libros están prestados y cuántos no, o detectar posibles robos.

Las posibilidades para quienes quieren controlar son ilimitadas, pero la sociedad civil ya se ha dado cuenta de las consecuencias. Lee Tien de Electronic Frontier Fundation ya ha puesto el grito en el cielo, afirmando que "las bibliotecas han sido tradicionalmente muy

respetuosas con la intimidad". Jackie Griffin, director de la Berkeley Public Library responde enérgico diciendo que "cuando era un adolescente dudaba si era gay o no, y no podía ir a una biblioteca y pedir prestado un libro sobre ello, porque otras personas podrían ver lo que estaba haciendo", mientras que con este sistema, el préstamo es automático, sin necesidad de que un bibliotecario tome nota de los libros prestados. Sin embargo, lo que descuida Griffin y apuntilla certeramente Katherine Albrecht, presidenta de la asociación CASPIAN[18] (Consumers Against Supermarket Privacy Invasion and Numbering), es que cualquiera con un lector de RFID corriente será capaz de leer los valores de los chips que portan los objetos que poseemos incluso fuera de su ámbito original, esto es, el libro seguirá devolviendo la señal de un lector RFID aunque se encuentre a kilómetros de una biblioteca, si ese lector RFID se situa lo suficientemente cerca, o un test-antiembarazo podrá ser detectado una vez fuera del supermercado por una persona que tenga un lector RFID y muchas ganas de investigar sobre la vida privada de alguien.

Como casi siempre, las situaciones de miedo extremo hacen que la sociedad permita perder parte de su libertad en favor de más seguridad. Esto se ha visto reflejado en un hecho insólito que relata el experto en Seguridad de la Información Bruce Schneier en su página web: después de los atentados del 11 de septiembre, la administración Bush ha puesto en marcha una medida mediante la cual los ciudadanos de países que actualmente no requieren de visado para entrar en los Estados Unidos de América deberán disponer de pasaportes que se ajusten a los nuevos controles de seguridad. Estos controles exigen que el pasaporte disponga de un chip RFID que informe en todo momento del nombre, apellidos, fecha de nacimiento y demás datos a la hora de accionar un lector RFID a menos de 10 metros de distancia del pasaporte [19]. Como comenta Schneier, los nuevos modelos de pasaportes sobre los que se estaba trabajando anteriormente también disponían de un chip con todos esos datos para agilizar su lectura, pero no era un chip de radio-frecuencia, era necesario pasar a través de un lector el pasaporte, como ocurre con las tarjetas de crédito. Es decir, el portador del pasaporte sabía cuándo se estaban leyendo sus datos y cuándo no. Con la nueva tecnología RFID esto no es así, en cualquier momento pueden estar leyendo los datos contenidos en el chip de su pasaporte sin que su portador lo sepa. Un agravante es que no solo los servicios de inmigración pueden hacer esto, sino que cualquier persona con la tecnología necesaria (un lector de RFID es algo barato hoy en día), puede leer esos mismos datos sin que nadie se entere aparentemente.

Las mejoras en la producción de estos chips espía han conseguido que se puedan fabricar en escalas inferiores al tamaño de una lente de contacto común, permitiendo su integración en casi cualquier producto. En 2003, Katherine Albrecht alarmó a la opinión pública al descubrir que en un supermercado de Cambridge de la cadena Tesco todas las cuchillas de afeitar Gillette poseían un chip RFID en su envoltorio y el stand donde estaban expuestas detectaba cualquier movimiento de su posición para hacer una foto de la persona que había cogido una cuchilla, como medida contra posibles robos de cuchillas. "No vamos a saber donde estarán esos productos etiquetados, y no sabremos tampoco cómo están siendo usados" manifestó por aquel entonces Albrecht. Horas después, las principales páginas web de noticias tecnológicas en Internet (slashdot.org o theregister.com, entre otras) arremetieron contra esta nueva tecnología que viola la intimidad de los consumidores[20].

El control no solamente se da a través de las ondas de radio, David Brin, escritor del best-seller “The Transparent Society”, alertó a finales de los 90 de la existencia de más de 150.000 cámaras de televisión distribuidas por todo el Reino Unido por la policía. Dado el bajo coste de esas cámaras, el autor calcula que actualmente rondará el millón de cámaras. Tal y como reza el cartel del metro de Madrid, “Más de mil cámaras velan por tu seguridad”. Una vez más, el trueque seguridad por intimidad, esta vez de forma tácita.

Hacktivismo

El hackitivismo es la fusión del hacking y el activismo, la utilización de las técnicas hackers para una causa política. Tal y como se explica en thehacktivist.com, el término hacker se utiliza en referencia a su significado original, es decir, una persona que disfruta explorando los detalles de sistemas programables y cómo ampliar sus funcionalidades, mientras que activismo se define como la práctica de la acción directa y militante para conseguir una meta social o política. Ambos términos están cargados de múltiples interpretaciones, por lo que definir hacktivismo se hace complejo y es necesario entender el movimiento hacktivista como en continuo cambio, evolucionando como un proceso abierto [21].

Los orígenes del hacktivismo fueron bastante funestos. Los hackers de comienzos de los 90 criticaron el hacktivismo por su uso dañino de la Red y sus técnicas primitivas, "sois peores que script-kiddies (niñatos que no saben hackear, pero copian programas que han hecho hackers para hacer daño en la Red), tecnológicamente patéticos" dijeron los hackers. Desde el activismo tampoco fueron vistos con buenos ojos, existía por aquel entonces un fuerte movimiento primitivista y neoludita que entendía la tecnología como un instrumento del poder, totalmente contrario a la lucha activista. Aún así, Ricardo Dominguez y otros hacktivistas cercanos a la Desobediencia Civil Electrónica siguieron trabajando en herramientas sencillas de usar, continuando con su idea de acercar herramientas de interacción tecno-políticas a la gente corriente. El ejemplo más claro de la aplicación del hacktivismo en sus inicios fueron las manifestaciones en la Red o netstrikes. Con un programa muy sencillo, utilizable desde cualquier ordenador personal, un hacktivista realiza continuas peticiones a una misma página web intentando colapsarla. Si este ataque se combina desde diferentes fuentes, se puede perjudicar seriamente la accesibilidad de un sitio web. El fundamento es similar al de congregar en la puerta de un banco a 200.000 personas para que traten de ser atendidas en la ventanilla de ese banco. Realmente no está ocurriendo nada ilícito, pero a efectos prácticos el resultado es que cualquier cliente "legítimo" de ese banco no podrá acceder a la ventanilla durante ese día, porque está saturada intentando atender a las miles de peticiones extra que se han generado con el ataque. Un caso sonado de manifestación en la Red fue el coordinado por la web italiana www.netstrike.it. En 1995 consiguió bloquear los sitios del gobierno francés que en aquel momento estaba bombardeando con cabezas nucleares el atolón de Mururoa[22]. Desde entonces una serie infinita de netstrikes ha sido realizados, en algunos casos promovidos por netstrike.it, en muchos otros casos a iniciativa de otra gente en todo el mundo. Seis años después, coincidiendo con las protestas contra el G-8 en Génova, el servidor de netstrike.it fue secuestrado por la Jefatura de la Policía de Bolonia, por orden del Departamento de la Policía Postal genovesa. Como comentaron los integrantes del grupo netstrike.it en un manifiesto

hecho público en la red, ha pasado ya mucho tiempo y, a pesar de la diligente atención de las fuerzas del orden, ningún juez, por más celoso de su tarea que fuera, ha pensado en ningún momento que pudiera procesar a alguien por esta práctica de lucha que tiene un valor exclusivamente simbólico y demostrativo. No sólo netstrike.it ha coordinado este tipo de manifestaciones en la Red o sentadas virtuales, la gente de hactivist.com también idearon sencillas herramientas para los navegadores web de la época con el mismo objetivo: visitar una misma página web de forma reiterada para evitar su acceso por otra gente. En este mismo sentido ha trabajado también el colectivo Electro Hippies.

Pero sus actividades no se reducen a unas cuantas protestas en Internet, la última hazaña de estos activistas hackers fue modificar una bicicleta para que, con la ayuda de unos brazos mecánicos y un ordenador portátil, pudiera hacer pintadas por las calles de Nueva York durante la última convención republicana. La bicicleta además disponía de conexión inalámbrica a la Red y utilizaba sprays de pintura no permanente, dado que en la ciudad de Nueva York los graffitis están prohibidos. Aún así, el inventor, Joshua Kinberg, fue arrestado. A las pocas horas fue liberado, pero su proyecto de bicicleta, que incluye ordenador, teléfono móvil y red inalámbrica, continua requisada[23].

Otro golpe de efecto grande lo protagonizó el colectivo The Barbie Disinformation Organization, un grupo de hacktivistas californianos que a principios de los noventa compraron muñecas Barbie y muñecos guerreros G.I.JOE que reproducían frases predefinidas. Una vez descubierto el mecanismo mediante el que se reproducían esas frases, intercambiaron los discos de los dos tipos de juguetes, obteniendo Barbies que decían "¡La venganza será mía!" y muñecos G.I.JOE que preferían decir "¡Planeemos la boda de nuestros sueños!". Con un cuidado exquisito, volvieron a colocar a los muñecos en sus envoltorios y devolvieron los juguetes a los grandes almacenes. Una vez descubierta la acción reivindicativa, el colectivo The Barbie Disinformation Organization declaró irónicamente que todo había sido beneficioso, "los dueños de los grandes almacenes vendieron dos veces el producto, estimulamos la economía, y nuestro mensaje se escucha[24]".

Re-code, un proyecto de hactivist.com, también tiene como objetivo prioritario los grandes almacenes. Gracias a su labor de ingeniería inversa, conocen cómo se codifica, en códigos de barras u otro tipo de codificación, la información acerca de un producto. Utilizando estos conocimientos son capaces de generar nuevas etiquetas para sustituir la codificación original de los productos de marca por productos similares sin marca. Con esto se pretende hacer una crítica ácida a las plusvalías asociadas a productos solamente por cuestiones de publicidad e imagen, tratando de sembrar el caos en grandes superficies que dependan de la automatización del proceso de facturación de una compra. Actualmente este proyecto está congelado, debido a las numerosas presiones que ha sufrido para que abandone su práctica y la distribución del material necesario para que estos ataques se repitan por todo el mundo, a pesar de que no han podido ser acusados de vulnerar ninguna ley hasta la fecha.

El software libre como herramienta para el hacktivismo

Con el uso del Software Libre como uno de sus pilares fundamentales y en paralelo con la actividad hacktivista desarrollada sobre todo dentro de los países anglófonos, surge el movimiento de hacklabs a finales de los años 90 en Italia. En el año 1998 se convocó en

Florencia el primer hackmeeting italiano[25], pretendiendo reunir en él a hackers, hacktivistas y artivistas (activistas del arte) para compartir impresiones, realizar talleres u organizar acciones conjuntas. Dado el éxito de la convocatoria, se decidió repetirla de forma anual y desde esa fecha se han venido produciendo hackmeetings cada año en diferentes partes de la geografía italiana. Gracias a la cohesión y organización surgida de cada uno de estos encuentros, los hacktivistas italianos se han ido organizando en hacklabs, laboratorios de hackers, o más bien hacktivistas, con un marcado carácter técnico y político, en continua sinergia.

Debido a la intensa interacción entre el movimiento telemático antagonista de Italia y de España, el fenómeno del hackmeeting se exporta a Barcelona en el año 2000. El Centro Social Ocupado Autogestionado Les Naus acoge la primera edición de un encuentro que desde entonces no ha hecho sino crecer en cuanto al número de sus asistentes y de actividades organizadas durante el mismo. Los hackmeetings han servido también para ir generando, en las ciudades donde ha tenido lugar, grupos locales más o menos fuertes que han derivado en la creación de hacklabs. Así, en Barcelona surgió el hacklab Kernel Panic[26] tras el hackmeeting, y al año siguiente el hackmeeting se trasladó al Gaztetxe de Udondo en Leioa, cerca de Bilbao, creándose el hacklab Metabolik[27] semanas después. En 2002 el hackmeeting se organizó en el CSOA Laboratorio'03 en Madrid y para entonces el fenómeno de los hacklabs había proliferado en muchos lugares cercanos: Cielito Lindo[28] en Lavapies, el Kaslab[29] en Vallecas, y actualmente el PiLab [30] en el Barrio del Pilar o Barahacks[31] en Barajas. Otras ciudades sonaron entonces como futuras sedes del siguiente hackmeeting como Zaragoza con el hacklab Downgrade[32] o Alicante con La Cuca Albina[33]. Finalmente el cuarto hackmeeting se celebró en el recientemente derribado Gaztetxe Euskal Jai en Pamplona, gracias a la labor del hacklab navarro Hackresi[34]. El fenómeno de los hacklabs ya es imparable y se organizan nuevos grupos en Vitoria-Gasteiz (Kakelbont[35]), Parets del Valles (Tenes777 [36]), Galicia (A causa encantada[37], proyecto que ya años antes tenía una sensibilidad por la telemática antagonista) o Sevilla (Sevilla-Hacklab[38]), anfitriones de la última organización del hackmeeting, durante el puente de Todos los Santos de 2004 en el CSOA Casas Viejas de Sevilla.

Como hemos podido observar, el movimiento hacktivista asociado a los hacklabs[39] y los hackmeetings tiene una fuerte relación con el movimiento de ocupación y, quizá, con el movimiento anarquista. Esto no es algo fortuito, como comenta Azalai, hacktivista madrileña, "para mí, tanto los hackmeetings como los hacklabs representan una interesantísima y fructífera tensión-interacción entre lo social, lo tecnológico y lo político, y nacieron con la idea de integrar y contaminar mutuamente a gente de estos campos, y aprovechar las sinergias específicas de cada uno, guardando un equilibrio inestable necesario para hacer surgir lo mejor de cada uno de ellos". La filosofía hacker está muy en sintonía con la ausencia de barreras y de organizaciones jerárquicas que puedan entorpecer el libre flujo de la información. En palabras de Blicero, legendario hacker italiano, "la experiencia de los Centros Sociales Ocupados Autogestionados puede considerarse una especie de *reality hacking*, en tanto que están impulsados por el mismo afán de experimentación, construcción y deconstrucción autónoma de sistemas, en este caso más sociales que computacionales o tecnológicos".

Además de organizar eventos más o menos endogámicos, los hacklabs tienen una

vertiente muy social y eso se manifiesta en forma de proyectos. Con el software libre como bandera, los hacklabs organizan cursillos periódicos de formación sobre temas meramente técnicos como navegar por Internet, escribir correos electrónicos o instalar GNU/Linux en un ordenador o talleres con una vocación más activista como la creación de redes ciudadanas inalámbricas al margen de Internet, talleres de criptografía básica utilizando GnuPG, una herramienta libre de cifrado (como disponemos del código fuente de esta herramienta, ningún gobierno podrá introducir software espía o puertas traseras en ella, como ocurre con software privativo de Microsoft u otros fabricantes) o el uso de sistemas de navegación para evitar la censura de determinadas páginas web. Además pretender realizar una labor constante de concienciación social en temas relacionados con las nuevas tecnologías, entre los que destacan la lucha contra las Patentes de Software, que golpean en la línea de flotación del Software Libre, o la reivindicación de una socialización de la cultura y un cambio del modelo de explotación de la misma, fomentando licencias libres para la documentación o el arte como el movimiento Copyleft[40] o las licencias "Creative Commons"[41], un traslado de la idea de las tierras comunales (commons) al plano creativo.

Otra manera muy efectista de socializar la tecnología empleada por los hacklabs es el “Hacking The Streets”, también llamado en ocasiones “hack-in-the-streets”. Basados en los Reclaim The Streets que se han venido dando estos últimos años en las calles de Londres y del centro de Europa, los Hacking The Streets también pretenden reclamar las calles como lugares de experimentación político-tecnológica. Saquemos los ordenadores a la calle, acerquemos la tecnología a la gente normal, expliquemos todas sus posibilidades. El primer Hacking The Streets lo organizó Kernel Panic en el barrio de Gracia de Barcelona y causó mucha sorpresa entre la gente que transitaba por allí. Posteriormente otros hacklabs se han animado a organizar Hacking The Streets, algunos más sui generis como el realizado por los hacklabs madrileños dentro de un mercado, otros con gran éxito de público como el último realizado por Metabolik en la plaza de Unamuno de Bilbao, con dos carpas donde se impartieron talleres de redes inalámbricas, Software Libre en euskera, Indymedia, etc.

Los hacklabs dan en el centro de la diana al percatarse de que todas las medidas de control telemático a las que están sometidos pueden evitarse gracias al uso del Software Libre. Sería bastante ingenuo creer que las herramientas para luchar contra ese control van a venir de la mano del mismo sistema que controla. Comprar una aplicación software de criptografía a una empresa que no proporciona el código fuente no tiene ningún sentido, ya que podrían introducir código espía o puertas traseras que permitieran a miembros de esa empresa y / o del gobierno saltarse las medidas de seguridad de esa aplicación en su beneficio. La falsa seguridad que pudieran proporcionarnos mecanismos criptográficos integrados en el Sistema Operativo Windows de Microsoft, por ejemplo, podría verse vulnerada al darnos cuenta de que todas las versiones de Microsoft Windows han pasado previamente por la Agencia de Seguridad Nacional estadounidense para hacerles los necesarios ajustes. Países históricamente paranoicos con su seguridad como la República Popular de China han optado por abandonar sistemas de software privativo, de los que no disponen el código fuente, en favor de una distribución de GNU/Linux basada en código abierto, permitiendo así a dicho gobierno controlar si otro gobierno está intentando introducir software espía o disminuir selectivamente las medidas de seguridad.

Disponer del código fuente de un programa es una condición sine qua non para prevenir posibles malos usos desde el poder. Así lo han entendido también finalmente empresas productoras de software como Microsoft o Sun, que permiten establecer contratos de licencia a determinados gobiernos para que puedan observar parte del código fuente de los sistemas que venden, sin opción a modificarlo. Es lo que se conoce como el Software Compartido o "Shared Source", o en lenguaje coloquial "se ve pero no se toca". Además, este tipo de licencias tiene el agravante de que no se aplican sobre todo el código fuente de una aplicación, sino solamente sobre una parte del mismo. Los hacktivistas ven esto como un engañabobos. Ninguna persona en su sano juicio podría asegurarse de que no lo van a envenenar si solamente le enseñan parte de los ingredientes del pastel, y si no le dejan la opción de tomar por su cuenta los ingredientes, la receta y cocinarlo en su casa para estar más seguro, cosa que sí es posible con el Software Libre.

Además de los ataques contra la intimidad personal, otra forma de control social se basa en crear corrientes de opinión a través de los medios de comunicación de masas. Los activistas de la Red pronto entendieron esto y durante las protestas antiglobalización de Seattle idearon lo que posteriormente se conoció como Indymedia[42]. Indymedia es una red descentralizada de servidores basados en Software Libre que proporcionan el sustrato físico para la red de Centros de Medios Indepedientes (IMCs) repartidos por todo el globo. En cada IMC se potencia que cualquier persona pueda informar y dar su punto de vista acerca de una situación o noticia. Siguiendo su lema "don't hate the media, become the media", pretenden aportar una nueva manera de informar y ser informado, sin censura, sin línea editorial y sin ideas preconcebidas. En Indymedia Euskal Herria, algunos hacktivistas de Metabolik BioHacklab, radios libres de la zona del Bidasoa y grupos afines han modificado el lema original: "Una persona, un reportero". La idea es que cualquier persona a pie de calle pueda sacar unas cuantas fotos desde su cámara y realizar una crónica contando lo que está sucediendo, sin el miedo al tijeretazo y con la cercanía que da que otro compañero cuente su visión de los hechos[43].

Desde Indymedia se ve un paralelismo claro entre las formas de actuar de los medios de masas convencionales, sus herramientas y sus estructuras. La CNN, por ejemplo, es un medio de masas unidireccional, que pretende crear corrientes de opinión muy diseñadas y dirigidas y que emplea una estructura interna claramente jerárquica. Además en el plano técnico utilizan tecnologías cerradas y software privativo que no permite que los visitantes de sus sitios web puedan contradecir las noticias emitidas. Por otra parte Indymedia es un medio de comunicación bidireccional, donde el rol de periodista y lector se mezcla en cada noticia, sin la pretensión de crear ninguna corriente de opinión ni de decidir por los demás qué es lo noticiable en cada momento, emplea una estructura organizativa horizontal y basa todas sus herramientas de publicación y gestión en el Software Libre. Esto le ha permitido no basarse en ideas preconcebidas de lo que era la Internet de hace 5 años e intentar que fuera posible que cualquier persona con la única ayuda de su navegador sea capaz de subir un video, unas cuantas fotos y varios documentos para contar una noticia, de forma sencilla y eficiente, y que ese mismo material esté disponible para todo el mundo de automáticamente cinco minutos después de haber pulsado el botón de "publicar".

Momentos importantes de las luchas sociales de estos últimos tiempos han podido seguirse con información de primera mano gracias a Indymedia y a toda la gente que ha colaborado con sus crónicas y comentarios: las protestas contra el pantano de Itoiz en Navarra, las reacciones a los atentados del 11-M, los desalojos de CSOAs en Pamplona, Barcelona o Bilbao, etc. Una vez más se ve como la lucha en la Red es una suma de activismo y tecnología, donde unos y otros aprenden día a día las posibilidades que ofrece el otro enfoque, de lo técnico a lo político y de lo político a lo técnico.

Conclusión

La lucha por los derechos y libertades civiles ha traspasado la barrera de lo virtual y los hacktivistas han sido los primeros en ser conscientes de ello. Las reacciones han sido diversas a ambos lados del Atlántico, mientras en los Estados Unidos de América las fuerzas se reúnen en torno a hactivist.com y sus originales proyectos de reutilización de la tecnología, en Europa el movimiento de hacklabs y hackmeetings ha constituido una red fluida de acción telemática culminando recientemente en la organización del Transhackmeeting Europeo en Croacia.

El Software Libre como movimiento se sitúa de forma transversal al hacktivismo, legitimándolo y potenciándolo, permitiendo que sea capaz de luchar de igual a igual con grandes corporaciones o gobiernos. Abastece de conocimiento al hacktivismo y actúa como manantial o repositorio, dotándolo de cantidades ingentes de materia prima para sus objetivos.

Si bien las nuevas medidas de cibercontrol social podrían fomentar entre el activismo político global un resurgimiento de las ideas neoluditas totalmente contrarias a la tecnología y un fortalecimiento de tesis primitivistas, los nuevos hackers políticos optan por tomar la sartén por el mango, emplear todas las posibilidades que brindan las nuevas tecnologías y entender la Red como un espacio en el que dar rienda suelta a todas aquellas luchas que antes sólo soñaron.

Abandonando discursos derrotistas ven como "Otro Software es Posible", y no solamente es posible, sino que ya está aquí, funciona e incluso es superior técnicamente a productos que han costado billones de dólares. La sinergia de miles de voluntarios lo ha hecho capaz, gracias a las posibilidades de la Red. El modelo bazar gana la partida al arquitecto de la Catedral. Los hacktivistas entienden mucho mejor la Red que sus adversarios, ¿sabrán aprovechar la ventaja?

Licencia

Referencias

- Barandiaran, X. (2003). "La tecnociencia como espacio político. hacia nuevas formas de organización e interacción de la producción tecnocientífica. v.1.0". URL: http://sindominio.net/~xabier/textos/pres/pres.pdf.
- Barandiaran, X. (2004). "Activismo digital y telemático. Poder y contrapoder en el ciberespacio v.1.1". URL: http://sindominio.net/~xabier/textos/adt/adt.html
- Blicero (2001). "Un espacio de construcción y deconstrucción. Conversación con Blicero sobre la experiencia del LOA Hacklab de Milán. (Por Aris Papathéodorou y Ludovic Prieur)". Multitudes, 5. Versión castellana traducida por Daniel Gil. URL: http://www.sindominio.net/labiblio/doc/loahacklab.htm.
- Casacubierta, D. "Carnivore FAQ. Privacidad". URL: http://www.spain.cpsr.org/boletin000c.php
- Critical-Art-Ensemble (2001). "Digital Resistance". Autonomedia. URL: http://www.critical-art.net/books/digital/.
- European Parliament (2001). "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))". URL: http://www.fas.org/irp/program/process/rapport_echelon_en.pdf
- García Mostazo, N. (2003). "La libertad vigilada". Ediciones B. ISBN: 84-666-1099-5. URL: http://www.libertadvigilada.com
- Oliver Lalana, A. Daniel. "La protección de datos personales en Internet, ¿un derecho fundamental virtual?". URL: http://www.unizar.es/derecho/fyd/prodatos/pdf/uned2.pdf
- Quirantes, A. "Echelon y la gran familia". URL: http://www.ugr.es/~aquiran/cripto/informes/info025.htm
- Roig, G. (2004). "Hackers: activismo político en la frontera tecnológica".
- Sádaba, I., Roig, G. (1998). "El movimiento de ocupación ante las nuevas tecnologías. Ocupas en las Redes". URL: http://www.nodo50.org/lecturas/okupas_en_las_redes.pdf. Texto publicado en libro "¿Dónde están las llaves? El movimiento okupa: prácticas y contextos sociales", (Coords.) Ramón Adell Argilés, Miguel Martínez López. Libros de la Catarata. ISBN: 84-8319-182-2.
- Sánchez Almeida, C. (2004). "República Internet". URL: http://www.sindominio.net/biblioweb/telematica/republica/

- Seebach, P. (1999). "The Hacker FAQ". URL: http://www.plethora . net/~seebs/faqs/hacker.html
- Stallman, R. (2004). "Software libre para una sociedad libre". Traficantes de Sueños. ISBN: 84-933555-1-8.
- Vidal, M. (2000). "Cooperación sin mando: una introducción al software libre". URL: http://www.sindominio.net/biblioweb/telematica/softlibre/.

Notas

[1] Driver es una palabra inglesa que se utiliza en informática para denominar a un pequeño programa que permite utilizar un dispositivo en concreto, como una impresora, un CDROM, una pantalla, etc.

[2] Un Sistema Operativo es la parte del software que convierte a nuestra máquina (hardware) en un entorno más amigable. Nos aísla de todas las complejidades propias de la circuitería interna, presentando al ordenador como algo relativamente sencillo de manejar.

[3] Como dice Richard M. Stallman, "el primer paso para poder utilizar un ordenador era prometer que no ayudarías a tu vecino. Se prohibía la existencia de una comunidad cooperativa. La regla hecha por los dueños de software propietario era: "si usted comparte con su vecino, usted es un pirata. Si desea algún cambio, ruéguenos para que lo hagamos nosotros"". Parece que el hecho de ayudar a un compañero es comparable a entrar por la fuerza en un barco y raptar o matar a sus tripulantes...

[4] Hackers entendidos tal y como se expresa en esa Biblia para hackers que es el "Jargon File" de Eric S. Raymond.

[5] "La Catedral y el Bazar" es un ensayo bastante famoso escrito por Eric S. Raymond en donde se explica que hay dos modelos básicos a la hora de afrontar un proyecto grande: el modelo Catedral, con su estructura jerárquica, su jefe de proyecto, arquitectos, aparejadores, jefes de obra, peones, etc.; y el modelo Bazar, en el que todo funciona como en un mercadillo: los comerciantes saben qué mercados están copados y en cuáles hay oportunidades. Nadie tiene que decirle a un comerciante que no venda calzado, ya se preocupa él de ver que ya existen 4 puestos de calzado, y colaborará con el rastrillo haciendo otra cosa o trabajando para los puestos existentes. Es un "organismo" que se autorregula, por así decirlo.

[6] Tal y como podemos ver aquí: http://news.netcraft.com/archives/web_server_survey.html, Apache (que es Software Libre) se mantiene estable en torno al 68% de cuota de mercado mientras que su principal competidor, el Internet Information Server (de Microsoft), se tiene que conformar con un 21% de cuota.

[7] Parafraseando a la mítica definición de Software Libre que proporciona la propia Free Software Fundation en http://www.gnu.org/philosophy/free-sw.html.

[8] El informe completo del Parlamento Europeo puede leerse aquí:

http://www.fas.org/irp/program/process/rapport_echelon_en.pdf.

[9] De esta misma noticia se hizo eco el diario digital IBLNews en julio de 2001: http://www.iblnews.com/news/noticia.php3?id=18939.

[10] El 3 de septiembre de 1999 la CNN hacía pública esta sospecha: http://www.cnn.com/TECH/computing/9909/03/windows.nsa/ y era ampliamente debatida en el foro de noticias tecnológicas Slashdot: http://slashdot.org/article.pl?sid=99/09/09/138209.

[11] http://www.cultdeadcow.com.

[12] Reconocido públicamente por el FBI: http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=25471.

[13] http://www.fbi.gov/programs/carnivore/carnivore.htm.

[14] Tal y como se puede leer en la declaración de privacidad de Passport .Net:

"Utilización de Su Información Personal.

La información personal recolectada en este Sitio será utilizada para operar el Sitio y proveer el/los servicio(s) o llevar a cabo transacciones que hayan sido solicitadas o autorizadas por usted.

Para soportar estos usos, Microsoft puede utilizar información personal para proveerle un servicio al cliente mas eficiente, para mejorar el Sitio o cualquier producto o servicio relacionado con Microsoft, y para hacer el Sitio mas sencillo de utilizar al eliminar la necesidad de ingresar una y otra vez a la misma información o para personalizar el Sitio a sus intereses o preferencias particulares."

[15] http://www.el-mundo.es/navegante/2003/12/10/empresas/1071058091.html.

[16] http://www.salon.com/tech/feature/2003/07/24/rfid/print.html.

[17] http://www.salon.com/tech/feature/2004/07/26/rfid_library/print.html.

[18] http://www.nocards.org/.

[19] Aparecido el 4 de octubre de 2004 en el International Herald Tribune: http://www.iht.com/articles/541711.html

[20] http://www.boycottgillette.com/index.html, http://slashdot.org/articles/02/11/17/0327244.shtml?tid=126, http://www.rfida.com/nb/gillette.htm.

[21] http://www.thehacktivist.com/hacktivism.php.

[22] http://www.sindominio.net/genova/textos/netstrike.html.

[23] http://www.boingboing.net/2004/08/29/rnc_protests_bikes_a.html.

[24] http://www.sniggle.net/barbie.php, http://www-2.cs.cmu.edu/afs/cs/user/jthomas/SurReview/reviews-html/bdo.html.

[25] http://hackmeeting.org/.

[26] http://sindominio.net/kernelpanic.

[27] http://www.sindominio.net/metabolik.

[28] http://sindominio.net/wh2001.

[29] http://vallekaslab.ath.cx.

[30] http://pilab.dyndns.org.

[31] http://barahacks.dnsalias.org.

[32] http://sindominio.net/zgz-hl.

[33] http://sindominio.net/lacucalbina.

[34] http://www.hackresi.net.

[35] http://kakelbont.org.

[36] http://tenes777.hacklabs.org.

[37] http://hacklab.causaencantada.org.

[38] http://sevilla.hacklabs.org.

[39] http://www.hacklabs.org

[40] En torno al copyleft y al procomún creativo o Creative Commons se ha articulado la web http://procomun.net.

[41] http://creativecommons.org.

[42] http://indymedia.org

[43] Los criterios de publicación de Indymedia Euskal Herria pueden leerse aquí: http://euskalherria.indymedia.org/static/es/editorial.html.