TESIS DOCTORAL

UNIVERSIDAD DE MÁLAGA, 2015

Facultad de Filosofía y Letras. Departamento de Historia Moderna y Contemporánea.

Grupos sociales y mentalidades colectivas en la historia moderna y contemporánea

PLÉCTICA DE LA SOCIEDAD DE LA INFORMACIÓN. *Internet como territorio de conflicto económico, social e ideológico.*

Doctorando

Francisco Andrades Galindo

Director

Emilio Ortega Berenguer

AUTOR: Francisco Andrades Galindo

http://orcid.org/0000-0001-8218-4250

EDITA: Publicaciones y Divulgación Científica. Universidad de Málaga

UNIVERSIDAD DE MÁLAGA | Departamento de Historia Moderna y Contemporánea

Emilio Ortega Berenguer, Prof. Doctor Titular de Historia Contemporánea del Departamento de Historia Moderna y Contemporánea de la Universidad de Málaga

CERTIFICA

Que la presente Tesis Doctoral, titulada

PLÉCTICA DE LA SOCIEDAD ACTUAL: CIENCIA, TECNOLOGÍA E IDEOLOGÍA EN LA SOCIEDAD DE LA INFORMACIÓN

Ha sido realizada bajo mi dirección por el Licenciado Don Francisco Andrade, y reúne el contenido científico suficiente y las condiciones necesarias para ser presentada y defendida ante el Tribunal correspondiente para optar al Grado de Doctor.

Málaga, 21 de Septiembre de 2015

Emilio O. Berenguer

UNIVERSIDAD DE MÁLAGA, 2015

Facultad de Filosofía y Letras. Departamento de Historia Moderna y Contemporánea.

Grupos sociales y mentalidades colectivas en la historia moderna y contemporánea

TESIS DOCTORAL

PLÉCTICA DE LA SOCIEDAD DE LA INFORMACIÓN. *Internet como territorio de conflicto económico, social e ideológico.*

Doctorando
Francisco Andrades Galindo

Director
Emilio Ortega Berenguer

PLÉCTICA DE LA SOCIEDAD DE LA INFORMACIÓN. Internet como territorio de conflicto económico, social e ideológico.

Indice

INTRODUCCIÓN: Líneas principales de trabajo

Internet no es el Futuro; es ahora. Una afirmación que nos sitúa en una realidad en la que seguimos llamando "nuevas tecnologías" a algo que lleva más de 30 años implantado, en un proceso que ha terminado por permear todas las capas de nuestra sociedad, la empresa, las formas de comunicarse, el propio concepto de educación y acceso a la información.

Tras la denominada sociedad de la información hay un proceso acelerado que nos conduce a una actualidad donde la tecnología interconectada es rutina dentro de las sociedades desarrolladas. Ya no se trata de un ordenador enlazado mediante una conexión telefónica analógica, condicionado por una infraestructura no creada con ese fin, ahora existe una conexión permanente y prácticamente ubicua que llega a la práctica totalidad de la población. Hablamos de una serie de servicios, como la mensajería móvil, más extendida ya que el propio servicio de telefonía fija convencional, de una información siempre disponible, de una realidad retransmitida en directo, inmediata y en buena medida opinable.

En un contexto en el que son muchos los puntos de vista, las líneas de trabajo, tratar de desentrañar la imagen prismática de esta complejidad, es una tarea prioritaria. Hemos recurrido a la imagen de una figura papirofléxica para poder explicar esta visión. La multiplicidad de "pliegues" que como una de estas figuras nos reporta la investigación, sobre cómo se ha configurado la realidad actual en el terreno de la sociedad de la información y las redes, se asemeja a tratar de conocer cómo está hecho esa figura "origami" *desplegando* en un plano todos y cada uno de los pliegues que conforman dicha "complejidad". La dificultad no es excusa

para que podamos hacer una aproximación de cuáles son los elementos fundamentales que han condicionado la evolución hasta el momento actual. Hasta el momento, se han producido varias aproximaciones desde diversas ópticas acerca de cómo hemos llegado a esta red que tenemos hoy en día. Trabajos como el de Matterlart o el de Castells, son referencia en cuanto a la descripción pormenorizada de los elementos destacados de nuestro tiempo en relación con la sociedad de la información. Nuestra idea, es la de realizar una prospección desde el plano histórico de una realidad que forma parte de nuestro ahora, pero sin dejar de lado los aspectos técnicos, aunque sea de forma descriptiva. Trataremos de sacar provecho de la trayectoria profesional del que escribe para poder aunar esta diversidad de aspectos y presentar una obra accesible pero con una narrativa que no omita ninguno de los aspectos principales que debe reflejar esta investigación. En esencia, haremos un sumario crítico del estado de la materia estudiada, algo tan reciente que forma parte de nuestro "ahora", pero que no por ello deja de estar sujeto a procesos históricos que podemos analizar, enumerar y criticar.

A lo largo del presente trabajo, hemos realizado un esfuerzo de contención para no excedernos en determinados puntos que por sí solos son terreno de amplio estudio, dado que la idea de éste es la de plantear una perspectiva de conjunto sobre un contexto en el que no existen este tipo de síntesis. Con esa misma idea, hemos titulado esta obra como pléctica, en alusión a la idea del científico Murray Gell-Mann, que trata de aunar el estudio de la complejidad en un plano simplificable.

Cuando explicamos qué es la sociedad de la información, cómo se ha formado Internet y todos sus servicios siempre se acuden a mitos e imágenes que por reutilizadas hasta la saciedad no dejan de ser recurrentes. Existen tres casos sobre los que deberíamos tratar cuanto antes para definir el perfil de nuestro trabajo: Cuando se habla de la "aldea global" y se parafrasea la idea de McLuhan, se apunta a una

concepción positivista y cándida de lo que es Internet hoy en día. Para ser realistas, la descripción de la red mundial de nuestros días se parece más al Chicago de los años 20', en diferentes niveles (con una visión no maniquea del asunto) en la que grandes empresas, cibercriminales y estados se disputan un espacio en el que las libertades individuales son las principales perjudicadas. Otra imagen manoseada hasta la saciedad es la del "mito fundacional", el "emprendedor de garaje". Si bien es cierto que muchos de los grandes éxitos de la red parten de unos orígenes modestos, y la "mitología del emprendedor" ha sabido abundar en el tema, la mayor parte de estos grandes éxitos también han partido de orígenes no del todo ejemplares, con no pocos "encuentros" con la legalidad correspondiente y desde luego con una ética pendiente de revisión. Por último, existe cierta tendencia a pensar que, una vez establecida la red, esta cuenta con unos parámetros fiables, completamente estabilizados y seguros. Nada más alejado de la realidad. Al igual que Richard Dawwkins explica cómo se organiza la evolución biológica (ya que vamos a utilizar imágenes) y nos detalla cómo el ojo humano es un agregado evolutivo, funcional pero chapucero, si hubiese sido diseñado realmente desde origen (solo hay que ver la posición del nervio óptico), Internet se ha formado mediante el mismo esquema de evolución; a partir de añadidos funcionales agregados desde diversos (a veces incluso contrapuestos) orígenes. Como vemos, todas estas ideas sobre la red y su funcionamiento pueden ser explicadas desde la óptica del conflicto, sobre la que queremos prestar especial atención en nuestro trabajo. Precisamente ésa será la tesis principal, por encima de ciertas explicaciones ya suficientemente documentadas para ser reproducidas, la del encuentro entre diversas ideas sobre la red y cómo cada una de estas se abre camino en la configuración de su estado actual. Una visión dinámica que encajaría en cierta medida en el análisis de la dialéctica clásica (contraponiendo tesis) aunque con muchos elementos en liza.

Como veremos, Internet es también cada vez más un entorno hostil sobre el que hay que tomar conciencia. La divulgación de herramientas de seguridad y el conocimiento público de errores y vulnerabilidades ha sido una norma entre la comunidad hacker. Esta publicidad, ha permitido que fallos de seguridad tenga un itinerario más breve y por tanto ha ayudado a mejorar los sistemas en general. Sin embargo, el paso a un modelo de negocio de muchos elementos de seguridad ha tenido una deriva perjudicial por una parte en el cibercrimen y por otra en la prestación de servicios a gobiernos y empresas con dudoso fondo ético y un gran secretismo. La restricción a la publicación de ciertas herramientas, con legislaciones como la alemana que prohíbe expresamente la tenencia de ciertos aplicativos (como el caso del famoso *Nmap o el escaneo de puertos en general*) e incluso la divulgación de su uso, por ejemplo mediante guías en la red, no hace más que propiciar la constitución de una red soterrada de información y la posesión de esta por parte de grupos restringidos. Así en lugar de propiciar el conocimiento y resolución transparente y pública de problemas de seguridad, se permite que grupos y entidades puedan explotarlos en beneficio propio, con finalidades mayoritariamente de espionaje o delictivas.

Con esta propuesta, pretendemos hacer una introducción a las complejidades y los diversos desarrollos concretos que se han sucedido a lo largo de los tiempos más recientes, en los aspectos sociales y económicos desde la perspectiva de las nuevas tecnologías y la organización de la red de redes, para llegar a concluir cómo la sociedad en la que vivimos en el presente no solo es una sociedad en transformación, sino que difiere sustancialmente de la que hemos conocido antes de este periodo entresiglos, de forma cada vez más profunda y que, a pesar de la proximidad en el tiempo, ya podemos apuntar multitud de aspectos diferenciales en una perspectiva bastante precisa. Desde que Francis Fukuyama (cita casi obligada cuando se habla de crisis postmoderna)

pretendiera el fin de la historia, hasta nuestros días se han sucedido suficientes acontecimientos diferenciales como para poder establecer un nuevo periodo diferenciado de esta. Nos encontramos con un periodo en el que no solo la sociedad actual ha cambiado de forma cada vez más acelerada, sino donde nuevos agentes y remozados elementos de otros más antiguos, han entrado de nuevo en juego para pasar a establecer las bases de un nuevo desarrollo social todavía en fase de rediseño.

En nuestro trabajo, pretendemos abarcar varios aspectos de esta complejidad sobre la que se teje el intrincado mundo actual, al menos desde el hito de la caída del muro hasta nuestros días. De este modo, rastrearemos los inicios de la denominada "*sociedad de la información*", para ver bajo que parámetros se ha gestado y que intereses subyacentes le sirven de impulso real. Creer por ejemplo, que la red de Internet que conocemos actualmente se trata de una caótica confluencia de nodos, sin tener en cuenta factores como la red de escuchas Echelon de la NSA estadounidense, o el ámbito militar en el que surgiera, será dar una respuesta superficial a la luz de las posibilidades de libertad que se han dado en ella, al margen de cualquier control y, precisamente por ello, capaz de un potencial creativo impensable hasta el momento.

Sin lugar a dudas, cuando hablemos de implantación de nuevas tecnologías o de avances en las ciencias, sobre todo en lo relacionado con la formación y desarrollo de la "red de redes" o puedan ser verdaderos factores de cambio social, elementos acerca de los que más nos detengamos en nuestro estudio, no podremos dejar de visualizar la tensión ideológica subyacente en todos estos campos; la forma en la que la propia estructura social y los diferentes agentes, que han confluido en la creación y desarrollo de Internet y las nuevas tecnologías en general, han tratado de marcar con su impronta estos elementos y cómo hemos tenido la suerte, en muchos casos, de que no hayan sido los presupuestos de control y de beneficio económico los que se hayan impuesto

completamente. En los terrenos de la informática se está dando una auténtica batalla entre ideologías totalmente contrapuestas. La concepción del Software Libre, teorizada por Richard Stallman, bajo la denominación de GNU, entra en conflicto directo con los intereses comerciales de grandes compañías. Precisamente, será esa lucha entre empresas que se pretenden propietarias de un material intelectual y los usuarios con conocimientos que ofrecen de una manera en gran medida altruista y colaborativa su trabajo, uno de los terrenos de muestra donde podemos ver cómo la sociedad postindustrial se adapta rápidamente a los cambios, cuando grandes corporaciones se convierten en adalides de una forma contrapuesta por principios a sus propias prácticas, por intereses confrontados a otras, con casos tan curiosos, conociendo su trayectoria, como el de IBM, adoptando Linux para encarar a Microsoft, como uno de los ejemplos más palpables. Por supuesto, el uso de la "legalidad" no deja de ser un instrumento más en esta disputa. Las tentativas de la UE de llevar adelante las patentes de software ha sido uno de los ejemplos más recientes de cómo se tratan de favorecer intereses particulares. Por contra, la adopción por parte del municipio de Colonia de software libre en todas las administraciones que gestiona, a lo que progresivamente de añadieron, con mayor o menos éxito, otras administraciones de diversos ámbitos en la UE y sobre todo en países con menos recursos, como es el caso de Brasil, nos demuestra como el interés general y la gestión en favor de la mayoría pueden darse también. El juego con la legalidad se ha utilizado también en campañas contra "la piratería", que ocultan los intereses y resistencias de unas compañías obcecadas en un modelo de producción cultural (en el que la cultura es un negocio totalmente dirigido) obsoleto, restrictivo y consciente de encontrarse en el final de una fase donde la propiedad física del soporte ha dejado de ser necesaria. Esta disputa, que contiene profundos tintes ideológicos, no deja de dar resultados curiosos, como por ejemplo, al rastrear la financiación de Microsoft, propietaria ahora de las cadena *CBS-NBC* en EEUU, a candidatos Republicanos y ver cómo estos luego acusan a los partidarios de sistemas operativos como Linux de

comunistas y obstruyen nuevas tentativas de reabrir los casos de monopolio de esta.

De cualquier modo, en nuestro trabajo no solo pretenderemos tratar sobre la sociedad de la información y la tecnificación acelerada, sino que pondremos el acento en el cambio de paradigma, político, económico y social de estos últimos tiempos. A la crisis de la postmodernidad, en la que muchos de los principios, sobre todo de una izquierda que se pretendía alternativa al sistema capitalista, no le ha sucedido ningún nuevo modelo ideológico que suponga contrapunto a los valores dominantes. De hecho, hemos podido comprobar cómo se está sucediendo un paulatino escoramiento hacia valores conservadores, reconocidos por la denominación anglosajona como "*Neocon*", que aúnan muchos aspectos de populismo conservador con la doctrina económica de liberalismo más extremo, en un proceso de pauperización del discurso político, tornado a espectáculo mediático, donde la convergencia ideológica tiende precisamente hacia un "pensamiento único", en palabras de Ramonet, en el que son escasos los márgenes para la diferencia, más simbólico-mediática que real . A la doctrina neoliberal entre los contrincantes de peso que se le conocen en el momento actual destacan los nacionalismos o el repunte de lo religioso, lo que significa el desastre de la alternativa. Resulta curioso, detenerse a analizar el papel de historiadores y filósofos en este aspecto en el que parece que no se han detenido tanto como se hiciera en otros momentos. En este sentido, el papel de científicos y divulgadores parece haber sustituido la influencia anterior de pensadores de otro tiempo. Es lo que G. Snow, definiera como la "tercera cultura", la confluencia de las culturas científicas y "de letras". Resulta curioso, por ejemplo cómo la respuesta más coherente al auge religioso en occidente la esté dando precisamente gente que provienen de campos ajenos, en principio, al fenómeno religioso. Así, al "Diseño Inteligente", idea con la que ciertas iglesias evangelistas de EEUU han tratado de remozar el concepto

de "creacionismo" para darle un tinte de relativa solvencia, llevando su labor "evangelizadora", en la que no faltan los intentos de anular la enseñanza de la evolución en las escuelas, a todos los aspectos de la sociedad, los que mejor han sabido responder han sido un genetista, Richard Dawkins, y un neurólogo, Sam Harris, hasta llegar a convertirse en referentes en el plano filosófico para los que defienden la independencia de las ciencias y el raciocinio.

Debemos reconocer que este será un proyecto que requerirá de una forma de trabajo distinta a la clásica archivística de un historiador. Sin embargo, esto no quiere decir que no se pueda elaborar desde una perspectiva histórica, sino que emplearemos fuentes y métodos diferentes y diversos en cada uno de los campos que tratamos de abarcar. Considero que es un tema interesante, desde el ámbito del historiador, tanto por tratar de analizar cuestiones muy recientes como por explorar una temática distinta, en la que quizás, al plantear cuestiones menos ligadas al estudio tradicional de la historia, menos se haya entrado a pesar de tratarse de una de las bases principales para entender el mundo en el que vivimos actualmente y ser los condicionantes claves para interpretar la trayectoria que diversos gobiernos y empresas, cada vez más unívocos en sus respuesta, tratan de inducir en nuestra sociedad cada vez más global y por otro lado más excluyente.

Desplegando la complejidad.

Con gran acierto, Laurence Lessing afirma que hay tres elementos que regulan la red: Los mercados, la ley y el código. El Internet que hoy conocemos es el producto de una serie de equilibrios entre diversas tendencias que buscan definir con su acción el futuro desarrollo de la red. De este encuentro de tendencias se forma este Internet que

tenemos en nuestros días, más preparado para ser persistente que seguro y fundamentado en el encuentro de los nodos que lo componen desde una multiplicidad difícil de homogeneizar. Una de las principales fuentes de este trabajo incide en esa lucha por imponerse, tanto desde el ámbito empresarial como desde el político, en proceso de convergencia. Convertir la red en un mercado de consumidores convenientemente dirigidos por estrategias comerciales y un poder capaz de malear las leyes a su favor es una de las líneas que apunta el presente trabajo. La resistencia a este formateo cultural, tanto expresada en el rechazo a leyes de patentes y derechos de autor, enfocadas hacia un interés que no es general, como en las nuevas formas de difusión cultural y creación alternativas plantean las primeras disyuntivas de nuestro trabajo.

El planteamiento del presente trabajo parte de una explicación necesaria del contexto para ir adentrándonos en el terreno de la confirmación de las hipótesis de trabajo que nos fijamos. Como podrá comprobarse la composición de esta obra no es simétrica. El peso principal y la mayor parte de la exposición de nuestras tesis recaen en los capítulos finales, especialmente en el bloque cuarto. La propia orientación del trabajo explica esta forma dado que los dos primeros capítulos son una obligada contextualización, en la que tanto sucesos históricos como ideas principales del trabajo son expuestos de forma concisa para fijar una panorámica general. A partir del tercer bloque, la materia debe concretarse y por tanto por encima de la "línea temporal" se impone la temática. También comenzamos a desgranar las conclusiones frente a la exposición de hechos. Todo el tercer bloque está dedicado a legislación sobre los derechos de autor y patentes y cómo la propia red ha planteado alternativas a un sistema que pretendía persistir en un modelo de negocio obsoleto. Las alternativas, tanto comerciales, como de licencia libre así como los modos informales de acceso a unos contenidos de otro modo restringidos, ya sea en forma de bloqueo como mediante la imposibilidad

económica son las principales ideas que se sugiere a lo largo de estos capítulos.

A lo largo del cuarto bloque de la obra, exponemos con mayor claridad los hechos que componen las tesis principales de nuestro trabajo. En ellos, se pasa al núcleo principal de nuestras tesis, la visión de la red como un territorio de conflicto en el que delincuencia, gobiernos y empresas buscan captar la mayor cantidad posible de datos de la ciudadanía de diversas formas. Las grandes revelaciones del espionaje ciudadano, pero también la forma de organizarse las redes sociales y su orientación comercial, condicionan de manera radical la visión de la red de nuestros tiempos. El proceso de toma de conciencia de la realidad que conforma Internet se encuentra en pleno desarrollo. El cambio de una realidad compuesta desde la visión inducida de la web 2.0 y las grandes presentaciones comerciales imbuido todo de un consumismo positivista, hasta la crisis económica y los cambios posteriores al 11-S en lo que respecta a libertades ciudadanas es todavía un proceso actual que todavía no ha llegado a su máximo alcance. La madurez de cada vez mayores grupos de activistas y ciudadanos ha venido acompañado de una expansión y popularización del uso de la red entre grupos mayoritarios de la población mundial, especialmente en entornos económicos desarrollados.

En las conclusiones se expone que una sociedad incapaz de elevar el ejercicio de sus derechos permite con su inacción el avance de las medidas de quienes diseñan su estrategia conociendo perfectamente este hecho. También se apunta cómo mantener a la ciudadanía en un estado de vigilancia permanente por la eventualidad de un compartimento delictivo no es solo un atropello a las libertades sino una auténtica declaración de intenciones de quien tan solo lo sugiere. Las fuentes de los problemas de la sociedad actual no se resuelven mediante el espionaje ciudadano. El

estado de madurez por venir puede significar retomar la soberanía individual y colectiva sobre nuestras vidas o una cesión al modelado social.

Resulta inevitable, incluso en un trabajo científico, una vez expuestos los elementos que conforma la cuestión analizada, no formarse una opinión y tomar opción, especialmente cuando se hace imposible la identidad con ciertos elementos de la disyuntiva. Así, tanto desde el compromiso como desde el conocimiento de la materia expuesta, la opción del que escribe siempre será la del partidario de la transparencia, de una visión basada en la opción democrática, la opción de la pastilla *roja.*

I: Orígenes de la Sociedad de la Información

Definiciones y conceptos previos

Bajo la denominación de "sociedad de la información" se han agrupado múltiples conceptos y pretensiones diversas e incluso contradictorias a veces. Pensar que la sociedad de la información, el mundo de las tecnologías y más concretamente todo lo que hacer referencia a la red, es ese mundo aséptico, carente de intencionalidad, que se movería como una especie de entidad caótica que se autoorganizara gracias a la confluente acción de empresas y usuarios, resulta ser el entorno ilusorio, el escaparate ficticio en el que muchos han cimentado las esperanzas de una nueva sociedad, en la que el avance de las nuevas tecnologías marcara las pautas, al margen de ideologías o controles. La realidad es bien distinta y los primeros indicios de esto podemos encontrarlo en la intencionalidad inherente de los propios términos con los que se tratan de definir los conceptos claves en los que se maneja la organización de esta pretendida sociedad emergente. Como certeramente afirma Armand Matterart[1] "*el mercado de las palabras queda reducido a las palabras del mercado"*, y la uniformación del mundo comienza en las palabras que empleamos para designarlo.

Sin lugar a dudas, cada modo de producción, cada sociedad, trae consigo una forma particular de establecer un ideario, una forma de identidad cultural entorno a la que se justifica. De este modo, la transformación de la sociedad capitalista, tal y como la hemos conocido a lo largo del siglo XX, hacia un modelo de desarrollo basado en la

[1] *Matterart, A .Historia de la sociedad de la información*. Paidos: Barcelona. 2007

información, las comunicaciones y el poder basado en dispositivos electrónicos, se ha deslizado, de modo casi imperceptible durante el periodo de *entresiglos*, para apuntar hacia una profunda transformación del poder y la forma de ejercerlo. Una transformación, por otro lado, que acentúa las desigualdades regionales, a pesar de que la pretendida "aldea global" unificaría, más allá de las regiones, la cultura y el poder. La realidad es que los centros de poder, bajo una óptica exclusivamente mercantilista, bajo las directrices de la doctrina neoliberal, se han concentrado más aún entorno a grupos de poder cada vez con menor identidad nacional pero, tal vez por ello, más poderosos. Esa carencia de identidades, de ideologías fuertes y atractores colectivos, propios de la crisis de la postmodernidad [2] , se ha convertido en uno de los signos definitorios de nuestro tiempo, "vaciado" de utopías y alternativas sistémicas que no provengan de un ámbito idealizado de lo tecnológico, bajo cuya pretendida asepsia funcional se socavan los principios de lo público. La relativización y frivolización, la saturación de "información no deseada", en palabras de F. Machup, llevara con el tiempo a producir una transformación social y cultural en unos términos dirigidos y controlados de una manera que por sutil, es la más profundamente radical de toda la historia de la humanidad. De este modo, grupos concretos de comunicación como AOL- Time Warner Media, Disney, Sony, News corporation; Viacon y Bertelsmann, controlan el 70% de toda la producción audiovisual mundial, imponiendo unos roles estéticos y culturales mediatizados[3] .

---

[2] Martín-Barbero, J. *Tecnicidad, identidades, alteridades: desubicaciones y opacidades de la comunicación del nuevo siglo*. En Sociedad Mediatizada. Gedisa. Barcelona.2007.

[3] McLuhan, M. *La galaxia Guttember: génesis de homo tipographicus.*Círculo de lectores, Barcelona. 1998.

Como afirmara Marshal McLuhan, "el medio es el mensaje"[4], los contenidos han perdido sentido respecto a la tiranía de la forma, el imperio de la imagen y la nueva semántica de la información, en el que la tecnología y la ciencia son la nueva ideología, en una suerte de nuevo positivismo carente de competencia. En ese aspecto, las únicas respuestas organizadas que han quedado, ante este proceso de desarraigo de lo colectivo y carencia de identidad, han sido las construcciones realizadas de lo excluyente y las religiones cada vez más sesgadas y con rasgos cada vez más fundamentalistas. En este sentido, cabe hacer mención, a modo de curiosidad, cómo en los EEUU, cuando se propusiera la reserva de un tercio de la programación por cable para usos de organizaciones comunitarias, recayeran la práctica totalidad de ellas en iglesias evangélicas, sus organizaciones aledañas o directamente telepredicadores[5] .

En este contexto, podríamos ir adelantando conclusiones respecto a los motores del nuevo paradigma social, aunque sin perder la perspectiva que nunca han sido las tecnologías las que impulsaran los cambios sociales por definición, sino que han sido elementos potenciadores, impulsos concretos a estas transformaciones; al igual que la máquina de vapor no trajo necesariamente la sociedad capitalista, tal y como se organizara, las nuevas tecnologías de la información y la comunicación, tampoco son, por si mismas, los agentes del cambio social, sino parte del entramado, político, económico y cultural que en su conjunto supone un modelo diferente al que conociéramos un par de décadas antes. En esta nueva sociedad en permanente gestación, en transformación incesante, podemos puntuar nuevas pautas sociales, diversas formas de

---

[4] *Óp. cit (2)*

[5] *Óp. Cit 1.*

interacción del individuo con la sociedad y el poder, entendido como la auténtica fuente de cambio y dirección social más que como gobierno representativo o dirigente.

Ese cambio social podría ser resumido en la transformación del *ciudadano* al espectador/consumidor, como forma concreta de resumir esta nueva aldea global dirigida por la doctrina ideológica del liberalismo, con un cada vez mayor aislamiento social y una saturación de imágenes en información de supuesto carácter neutral, a pesar del sesgo evidente hacia la doctrina dominante. En definitiva, no deja de ser una nueva forma de hegemonía, en términos gramscianos, característica básica de la "sobremodernidad" [6]

Por tanto, la forma en la que se impulsa el cambio social no es en ningún sentido todo lo aséptica que el positivismo "mainframe" (opinión mayoritaria), tantas veces convenientemente inducido, pretende explicarnos. Ante esto, existe una narrativa de resistencia que aúna a defensores del software libre, periodistas independientes, activistas y organizaciones no integradas en los engranajes del sistema que plantean una forma diferente de interpretar el cambio[7].

---

[6] . Augé, M. *Sobre modernidad: del mundo tecnológico de hoy al desafío esencial del mañana. En Sociedad Mediatizada*. Gedisa. Barcelona.2007

[7] Kleim, N. La doctrina del Shock. El auge del capitalismo del desastre. Booket. Madrid. 2012

1.2 Precursores de la red

El afán por simplificar, codificar y reducir a impulsos eléctricos computables en formato binario de apagado-encendido (0-1) cualquier comunicación, bajo un sistema lógico, es un principio que podríamos detraer al propio origen de la ciencia matemática y que, de hecho, ha sido una búsqueda de una simplificación del lenguaje, de una forma de codificación informativa, como tratara de hacer Leibniz[8]. , al hablar de un proceso de automatización de la razón, del *procesado* mental en algo sintético, reducido a sus formas básicas; es decir, el origen de un proceso sintético que surgiera en sus orígenes como búsqueda de una certeza matemática y que finalmente ha devenido en clave de todo el proceso de comunicación de nuestra época.

Gordon Moore[9] , directivo de la famosa compañía Intel, sintetizo lo que, en origen, podría tratarse de una ocurrencia sugerente, en toda una "ley" que de un modo u otro se ha convertido en una suerte de máxima de las compañías de fabricación de microprocesadores; la conocida como "*Ley de Moore*", por la cual la capacidad de tratamiento de información de todos los microprocesadores se duplica cada año y medio. Efectivamente, podemos ver como las creencias y convicciones de los promotores de este nuevo paradigma, terminan siendo condicionantes capaces de provocar efectos tangibles en la realidad. A nadie nos sorprende que a veces, sobre todo teniendo en cuenta que es la propia *Intel* la promotora de nuevas

---

[8] Matterart, A .*Historia de la sociedad de la información*. Paidos: Barcelona. 2007.

[9]. Moore, G.E. *"Progress in digital integrated electronics*", IEEE International Electron Devices Meeting, IEDM Technical Digest 1975, pp. 11-13

tecnologías de "duplicado" de procesamiento, ajuste las presentaciones al público de sus tecnologías al patrón de Moore[10] .

Curiosamente, y a pesar de la imagen relativamente romántica de unos jóvenes creando las bases de la informática en un garaje, la realidad ha sido bien distinta y, a pesar de la iniciativa concreta de jóvenes investigadores, sus inquietudes y su capacidad, el origen financiero de todos estos progresos se debe, como casi todos los grandes avances técnicos del siglo pasado, a los fondos públicos aportados en buena medida por el departamento de defensa del gobierno norteamericano que, en origen no tenía objetivos militares y, en realidad, no tenía más objetivos que los que le fueron dando sus propios investigadores y primeros usuarios.

Respecto a los orígenes de la red tal y como hoy en día la conocemos, existe una profusa bibliografía e incluso no resultaría nada complicado emplear la red y los instrumentos que esta nos ofrece para poder conocer algunas síntesis sobre sus orígenes, proceso más fácil aun cuando la mayor parte de sus protagonistas son empresarios o investigadores de éxito que continúan en primera línea en la actualidad, dado que el proceso que ha llevado a este nuevo paradigma tiene un origen relativamente reciente.

No hay red sin infraestructura distribuida

El origen de la red de redes, tal y como hoy la conocemos, está estrechamente ligado al procesamiento de la información, al origen mismo de los transistores, los medios de almacenamiento y procesamiento y

[10] http://www.computerhistory.org/semiconductor/timeline/1965-Moore.html

transmisión de la información. Podemos remontarnos a 1947, momento del origen del transistor, por parte de los investigadores de los laboratorios Bell, en Nueva Jersey, Bardeen, Brattain y Shockley, que les llevaría a ganar un Nobel de física por ello. Con este instrumento, se hizo posible el codificar impulsos eléctricos de un modo binario de interrupción-paso, lo que nos permite la codificación lógica de información y la comunicación con máquinas y entre estas mismas. Estos dispositivos, denominados semiconductores, debido a este proceso, comenzarían pronto a integrar miles (con el tiempo, millones) de transistores y pasarían a denominarse comúnmente chips. Sin embargo, hasta que no se pudo ensamblar en un material más adecuado, depurando el proceso de errores no pudo comenzar a comercializarse dotándole de un uso concreto.

El paso a la integración de la tecnología basada en el silicio, gracias a la investigación de Gordon Teal, integrado en 1953 al anterior equipo, posibilitaría el proceso de miniaturización de componentes fabricados con instrumentos de precisión. Todo esta conjunción, llegaría con la confluencia de diversas investigaciones sobre procesos planares e integración de microelectrónica, basada en el circuito integrado, idea de Jack Kilby, técnico de Texas instruments que lo patentara en 1957, aunque sería Bob Noyce, quien lo fabricara antes y lo llevara a una aplicación práctica; lo que provocaría una auténtica explosión tecnológica en el terreno, que llevaría a la multiplicación de semiconductores, abaratando los precios de esto, ante la posibilidad de fabricación den cadena, en torno a un 85% en tan solo tres años. En torno a la mitad de esta producción sería absorbida por los usos militares.

El siguiente gran salto cualitativo se dará en 1971, cuando el ingeniero de Intel, Ted Hoff, creara el primer microprocesador, lo que significaría integrar en un chip todo un ordenador, dando pie a poder trasladar e instalar en cualquier parte todo el procesado informático. Esto daría origen a un proceso constante de superación, integración y

militarización que sigue constante en nuestros tiempos a pesar de los límites que se han creído insuperables en diferentes momentos.

Para poder conocer este proceso, señalaremos cómo la potencia de los chips puede ser evaluada mediante tres características claves: la capacidad de integración, señalada por la mínima anchura de las líneas del chip, medida en micras (millonésima parte del metro); su capacidad de albergar memoria, expresada en bits (kbit, miles, Megabit, millones) y la velocidad del microprocesador, expresada en megahercios. De este modo, podemos sopesar el avance conocido, expresado en el crecimiento exponencial de las capacidades concretas, viendo cómo el primer procesador de 1971, contaba con unas líneas de unas 6,5 micras, en 1980 eran ya de 4 micras, una micra en 1987 y en 1995, el chip Intel Pentium contaba ya con 0,35 micras. De este modo, donde en 1971 se podían insertar 2300 transistores en un chip del tamaño aproximado de una chincheta, en 1993 contaba ya con 35 millones de transistores. Respecto a la memoria, expresada en DRAM (Dinamic Ramdom Access Memory), mientras en 1971 era de 1.024 bits, en 1993 era de 1.024.000. Con la velocidad ocurre lo mismo y los procesadores de mediados de los noventa eran ya 550 veces más rápidos que los primeros de los setenta, ajustándose de manera férrea a la citada "ley de Moore" y su duplicación de velocidad cada 18 meses [11] .

El descenso en los precios de los microchips, su paulatina miniaturización y generalización en su uso, que cada vez se extiende a campos mayores, hasta constituir el componente de mayor precio en los automóviles a partir de la década de los 1990, se ha convertido, de este

[11] http://www.computerhistory.org/semiconductor/timeline/1965-Moore.html

modo, en uno de los procesos básico para conocer el periodo más reciente de nuestra sociedad industrial[12] .

De cualquier modo, los primeros ordenadores, al menos con la matriz reconocible hoy en día como tales, son hijos, como tantas otras tecnologías, de la segunda guerra mundial, como el *Colossus* británico de 1943, dedicada a descifrar los códigos enemigos [13] o el *Z-3* alemán producido para asistir los cálculos de rutas aéreas de sus bombarderos) [14]. En 1946, fruto de un programa de investigación del MIT (*massachusset institute of tecnology*), uno de los grandes referentes de todo el progreso tecnológico de nuestro tiempo, y el patrocinio del ejército estadounidense, surgiría en la universidad de Pensylvania ENIAC (Electrónical Numérical Integrator and Calculator), el primer ordenador propiamente dicho con fines generales. Un precursor de 30 toneladas, construido en módulos metálicos de 2 metros y medio de alto, constituido por 70.000 resistores y 18.000 tubos de vacío, con un consumo eléctrico que, en su momento, hacia resentirse la red eléctrica de Filadelfia al entrar en funcionamiento.

Seis años después, el mismo equipo técnico, bajo la marca Rémington Rand, produciría el primer modelo comercial del producto, denominado UNIVAC-1, que cosecharía su primer gran éxito en el procesado del censo estadounidense de 1950. En 1953, con apoyos similares, financiación por parte de contratas militares e investigación por parte del MIT, IBM entraría en la carrera informática con su máquina de tubo

---

[12] Manuel Castells. *La era de la información: economía, sociedad y cultura (Vol. 1): La sociedad red.* Alianza editorial. Madrid. 2008

[13] http://www.codesandciphers.org.uk/lorenz/colossus.htm

[14] Rojas, Raúl (1998). «How to make Zuse's Z3 a universal computer» *IEEE Annals of the History of Computing* (documento completo en: http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=707574#)

de vació 701. Así al *Mainframe (nombre que hace referencia a las cajas metálicas en las que se aloja)* desarrollado por Sperry Rand en 1958, IBM, contestaría con su propio modelo 7090, aunque no lograría la posición dominante que se le reconocería posteriormente hasta su *mainframe* 360/370, de 1964, momento a partir del cual en un proceso de "destrucción creativa" fiel a la descripción de Schumpeter, dejaría a la empresa en una posición de dominio casi absoluto de la industria informática [15] durante una época de relativa estabilidad en la producción de máquinas, con fines concreto y dirigidas a un mercado específico.

Hasta la introducción del microchip en las máquinas de procesado; en concreto hasta llegar en 1971 a poder ubicar lo que hasta entonces era un ordenador en un chip no llegaría el gran salto. Bajo el curioso nombre de Altair (un personaje de la serie Star Trek), Ed Roberts construiría en 1975 una caja de cálculo en torno a un microprocesador, un ordenador a pequeña escala que sería la base del diseño del Apple I luego del Apple II, el primer microordenador que se comercializaría con éxito; producto del trabajo de dos jóvenes, Steve Wozniak y Steve Jobs, que habían abandonado los estudios para realizar en los garajes de casa estas máquinas que se han convertido en el auténtico mito fundacional de la era de la información. En 1976, con tres socios y 91.000 dólares de capital, nace Apple computers, primera compañía en vender ordenadores como producto de consumo, que en 1992 ya había llegado a los 583 millones de dólares en ventas. La reacción del gigante IBM sería la presentación de su propio microordenador, bajo el nombre de Ordenador Personal (PC, Personal Computer), que sin embargo, al partir de desarrollos no

[15] . Manuel Castells. *La era de la información: economía, sociedad y cultura (Vol. 1): La sociedad red*. Alianza editorial. Madrid. 2008

elaborados por la propia empresa sino por otras fuentes diversas, se volvería vulnerable al clonaje, el versionado a partir de desarrollos fuera de la matriz, hecho que sucedería casi de inmediato a escala masiva, sobre todo en Asia, después de que Columbia Data Products clonase exitosamente la BIOS del IBM. Este hecho, llevaría a una difusión mayor, debido al abaratamiento de costes de máquinas *clónicas*, del modelo PC, frente al de las máquinas Apple, pese a su superioridad técnica. De hecho, volvería a ser el Macintosh de Apple, lanzado en 1984, el primer ordenador en comenzar a emplear una interfaz más accesible al usuario, fuera de la consola de comandos, con el empleo de iconos en un panel visual, desarrollada originalmente en el Centro de Investigación de Palo Alto de Xerox.

La vida en la máquina. La popularización del software para PC

Llegados a este punto, alcanzamos el segundo gran hito para la popularización de la informática y su extensión. El software, como elemento básico de uso e interactuación con la máquina (hardware). Efectivamente, el éxito de la máquina Altair llevaría pronto a otros dos jóvenes, que también abandonaran sus estudios en Harwad, Bill Gates y Paul Hallen, a adaptar el lenguaje de programación BASIC (Beginners All-purpose Symbolic Instruction Code) a esta máquina, creando el Altair Basic, primer producto de la compañía Micro-Soft (Microsoft hoy en día).

En 1981, la compañía recibiría el encargo de IBM de implementar un sistema operativo a sus máquinas PC. Con ese fin, Microsoft compró a Seattle Computer Products un clon de CP/M llamado 86-DOS, que IBM renombró como PC-DOS. Precisamente, la posibilidad de ser clonados de los PC de IBM, con el sistema operativo MS-DOS (Microsoft-Disk Operating System) como plataforma sería el acicate definitivo para el éxito de una compañía que, en principio surgiera como pequeño proveedor de software

(incluso más bien como adaptador de este). Así, a pesar de que la interfaz de usuario y la propia máquina desarrollada por Apple era superior y de más fácil manejo, la popularización de un modelo de menor precio comenzó a imponerse y los MS-PC se convirtieron en casi un estándar, sobre todo cuando Apple decidiera no licenciar ni permitir otros desarrollos de su sistema ni sus máquinas por parte de terceros.

En 1985, Microsoft lanzó Windows, su propio sistema operativo gráfico. Su primera versión, la 1.0, un desarrollo a medio camino entre una evolución gráfica de MS-DOS y un clónico de Mac OS, cosecharía su primer gran fracaso. Pero con la versión 3.1, Windows se consolidó y a pesar de las trabas legales que comenzaría a cosechar por sus prácticas comerciales, terminaría por imponerse como sistema casi universal de los PC (con cerca del 90% del mercado hasta la primera década del siglo XXI) [16].

No sería hasta la masiva adopción de comunicaciones entre ordenadores personales y la expansión de la movilidad en las redes cuando comenzaría a decrecer dicho liderazgo. El resurgir de Apple tras el retorno de Steve Jobs a la compañía y su acertada campaña de extensión de dispositivos, comenzando con los primeros iPod y luego con el iPhone. Las *Keynotes* de Apple (presentaciones anuales de mejoras y productos) se han convertido en una liturgia consumista en la que medios y comunidad de usuarios-consumidores asisten en directo a estas a modo de gran evento a escala mundial[17].

---

[16]. Un buen análisis sobre la posición de mercado de cada tipo de ordenador podemos encontrarlo en: http://arstechnica.com/old/content/2005/12/total-share.ars/10.

[17] . Isaacson, W. *Steve Jobs*. Trinith & Banshee. NY. 2011

La universalización del uso de la tecnología móvil o portable, entendida en un sentido extenso, propiciará la definitiva expansión de la red a una escala generalizada en las poblaciones de los países desarrollados y en buena medida también propiciará la penetración de las comunicaciones y el acceso popular en otras naciones, incluso a pesar de la censura de estados como el iraní [18]. Los casos de censura en la red tendrán especial relevancia [19], dado que jugarán un papel muy importante en situaciones de convulsión social como los de la denominada de forma generalizadora "Primavera árabe". Otro de los casos más destacados es el de China y su "gran cortafuegos" que prácticamente bloquea las comunicaciones fuera de su red. De un modo u otro todos los estados han comenzado desde principios del presente siglo a prestar una especial atención al nuevo escenario que se presenta con esta nueva expansión y popularización de unas comunicaciones no centralizadas ni dirigidas[20]. Como veremos más adelante, la intervención y la vigilancia tomarán un papel predominante en la evolución de las diversas agencias de inteligencia estatales.

[18]18. http://es.globalvoicesonline.org/2015/05/21/iran-en-medio-del-debate-por-la-censura-inteligente-el-gobierno-afirma-que-facebook-permanecera-bloqueado/

[19] 19. Una extensa entrada de la Wikipedia trata sobre el caso particular de la censura en irán http://en.wikipedia.org/wiki/Internet_censorship_in_Iran

[20] 20. Sobre la censura y la maduración de ciudadana: El fin de la inocencia en la red: http://andradesfran.com/el-fin-de-la-inocencia-en-la-red/

1.3 Nacimiento de la red

Tratar sobre el origen de la red de redes y su desarrollo es volver a situarnos en primer lugar en el contexto de la guerra fría y por otro lado en el de conocer los grandes difusores de sus capacidades para el público general, en este caso por parte de estudiantes y desarrolladores en general pero en todo caso sin ánimo de lucro, con fines científicos y con una concepción que resulta curiosa y radicalmente diferente a las tentativas de los que se han obstinado en convertir en negocio cuestiones que, en principio no lo fueran en absoluto. De este modo, podemos sugerir que el nacimiento de la red como hoy se conoce es el producto de la confluencia de factores diversos, la convergencia de los intereses militares, con su financiación, la cooperación de grupos científicos, en ocasiones con individuos ligados a la contracultura y el interés de diversas corporaciones.

La red de redes, como se conoce en muchas ocasiones a Internet y todos los servicios que la integran actualmente se debe tanto a un proceso de confluencia de intereses comerciales y militares, como a la desinteresada aportación de grupos de investigadores, usuarios y activistas en favor de una libertad todavía en disputa [21] . Un terreno que no difiere del de la misma participación democrática activa. La propia red se ha creado enmarcada dentro de ese estado de tensión entre tres vértices que

[21] Manuel Castells. *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*. Plaza & Janes. Barcelona. 2001

contienen puntos de partida divergentes a propósito de cómo tiene que ser Internet, sobre cómo debe gestionarse y sobre que parámetros [22] [23].

Como veremos, esta tensión subyacente se manifiesta tanto en la confluencia de intereses, como cuando investigación civil y militar colaboran, antes de hacer de Internet un gran negocio, como finalmente ocurre. Ya hemos adelantado que nuestro estudio, más que el mero relato de avances técnicos, ampliamente documentado, se va a centrar en las diferentes tensiones sociales [24] y políticas que se producen y condicionan la manera en la que la red de redes se conforma en la actualidad[25]. Por ello, serán varias las ocasiones en las que este relato se vea acotado por apreciaciones de este tipo, dado que el estado actual ha sido condicionado por la evolución para nada aislada de los elementos que la conforman.

El auge de la "nueva economía" dominada por la doctrina neoliberal[26], convertirá el eje comercial en el dominante[27], hasta el punto de infiltrar la investigación militar y en general de las agencias de inteligencia de los estados y dejará en el terreno de la resistencia y el activismo a la investigación independiente y las comunidades

---

[22] Manuel Castells. *La era de la información: economía, sociedad y cultura (Vol. 1): La sociedad red*. Alianza editorial. Madrid. 2008.

[23] Armand Matterart .*Historia de la sociedad de la información*. Paidos: Barcelona. 2007

[24] Marshal McLuhan. *La galaxia Guttember: génesis de homo tipographicus*.Círculo de lectores, Barcelona. 1998.

[25] Brockam, J. *La tercera Cultura. Más allá de la revolución científica*. Tusquets. Barcelona. 1996.

[26] Marc Augé. *Sobremodernidad: del mundo tecnológico de hoy al desafío esencial del mañana.* En Sociedad Mediatizada. Gedisa. Barcelona.2007.

[27] Jesús Martín-Barbero. *Tecnicidad, identidades, alteridades: desubicaciones y opacidades de la comunicación del nuevo siglo*. En Sociedad Mediatizada. Gedisa. Barcelona.2007

de investigadores independientes[28]. Comunidades científicas como las que publican en *Plos*, que ofrecen acceso libre a las publicaciones científicas o la más conocida Wikipedia son ejemplos de esta evolución[29].

Todos estos aspectos serán detallados más avanzado nuestro estudio pero deben tenerse en cuenta para comprender y ubicar la manera en la que se producen muchos de los avances de los que hoy en día disfrutamos.

Enlazando máquinas

A la hora de establecer la fecha concreta del nacimiento de Internet no existe un consenso completo, aunque si existen ciertos hitos que son comunes y que en su conjunto nos dan una idea de cómo se gestó.

Una de las primeras referencias por escrito, fuera de la ciencia ficción, a un sistema de comunicación de banda ancha entre máquinas, la encontramos en un escrito de 1960 por parte de J.C.R Licklider[30] . Efectivamente, será este mismo quien se encargue dos años después de la oficina de procesado de información de DARPA (Agencia de Proyectos de Investigación Avanzados de Defensa DE EEUU). Todas estas investigaciones culminarían en 1969 con la creación de la primera red sin nudo central, sobre un sistema de conmutación de paquetes de información denominado DARPANET. Como describiremos en el capítulo 1.5 *Ciencia, Universidades e Información,* la participación de varias instituciones

---

[28] . Ramonet, Ignacio. *Pensamiento único y nuevos amos del mundo*. Icaria. Barcelona. 2008

[29] Assange, J*. Cypherpunks. La libertad y el futuro de internet*. Deusto. Madrid. 2014.

[30] http://groups.csail.mit.edu/medg/people/psz/Licklider.html -1960

universitarias serán claves para esta primera red de cuatro nodos entre la UCLA, la UCSB, el Stanford Research Institute y la Universidad de Utah[31]. Será precisamente esta primera colaboración no militar la que promueva el cambio de denominación de esta primera red descentralizada por ARPANET en 1972[32].

Una vez establecidos los parámetros base para la red, protocolos hoy en día muy extendidos como el correo electrónico, cuyo primer programa fuera escrito en 1971 por Ray Tomlinson o el Protocolo de Transmisión de Ficheros (FTP), todavía tan vigente en la actualidad proporcionado ese mismo año por un grupo de investigadores del MIT, aunque no sería hasta 1985 que se publicara para su uso público.

En 1981 se terminará de definir el protocolo TCP/IP (Transfer Control Protocol / Internet Protocol), la base de todas las comunicaciones en red actuales[33]. ARPANET adopta este sistema en 1982. Al año siguiente se independiza de la red militar que la de la que surgiera, lo que potencia su extensión entre universidades e investigadores independientes[34].

En el otro extremo, suele ser una cita común la referencia al por entonces técnico del Centro Europeo de Física de Partículas (CERN) que a partir de un informe presentado en 1989 para mejorar el sistema de gestión de la información del centro. Esta será la segunda clave principal

---

[31] Breve diagrama sobre las primeras redes http://www.computerhistory.org/internet_history/

[32] Mapas de la distribución de ARPANET por años http://som.csudh.edu/cis/lpress/history/arpamaps/

[33] Ramonet, Ignacio *El control de Internet.* En *Le Monde Diplomatique*, 04/11/05

[34] Especificaciones del protocolo TCP/IP: http://www.rfc-es.org/rfc/rfc0793-es.txt

para la extensión de la red. La descripción de su lenguaje principal y el método de presentarlo y conectarlo. Nos referimos al método de transmisión HTTP (Protocolo de transferencia de hipertexto) y el lenguaje HTML (Lenguaje de marcas de hipertexto).

Sería el primer uso civil de una red informática y más aún, dado que los protocolos necesarios serían descritos de forma libre para que toda la comunidad dispusiera de ellos y extendiera esa interconectividad [35]. Estamos ante el origen de la red de redes. Una red abierta, con unos protocolos bien descritos y sin propietario, por tanto fácilmente adaptables y extensibles sin sobrecostes ni impedimentos. Dos años después, el mismo CERN[36] describiría el primer programa capaz de interpretar sobre la marcha los hipertextos: el primer navegador web.

Con la descripción del protocolo de transmisión de paquetes (TCP/IP), la forma de transferir texto mediante este (HTTP) y el lenguaje adecuado para verlo (HTML)[37] tenemos las bases sobre las que está construida nuestra red de redes. Todo ello producto de una serie de investigaciones abiertas, que en ningún momento restringieron el alcance de estas sino que por contra, difundieron de forma altruista o al menos no directamente interesada el producto de sus investigaciones para cimentar una red extensa que pudiera ser interpretada en cualquier lugar independientemente de la máquina. Esta apreciación es fundamental dado que estamos señalando que sin esta extensión las redes que se estaban creando hasta el momento habrían sido incompatibles entre sí, encerradas en el marco de sus propias organizaciones. Mención especial

---

[35] Cronología de las comunicaciones y precursores del corro electrónico: http://www.telecable.es/personales/carlosmg1/historia_correo.htm

[36] http://public.web.cern.ch/public/

[37] Especificaciones del HTTP del W3 consortium http://www.w3.org/Protocols/

tiene el método de *BBS* (Bulletin Board System -*Sistema de tablón de anuncios),* como la forma primigenia de comunicación entre redes de usuarios, precursora de los foros y los chats. En este apartado *Fidonet*[38], se convertiría en una de las primeras formas de comunicación directa entre usuarios y comunidades[39] con una extensión y una duración a lo largo del tiempo destacable.

A partir de 1995 el *WWW* se presenta como el primer servicio que saca provecho del primer navegador propiamente dicho, *Mosaic*, que había sido escrito dos años antes. A partir de esto y hasta el momento actual, las bases de la red mundial son las mismas, extendidas de manera uniforme a lo largo de todo el territorio mundial. Resulta particularmente esclarecedor cómo estas bases se han mantenida sustancialmente inalteradas y por ello mismo, muy a pesar de ciertas divergencias expresadas tanto por países denominados emergentes, como por democracias occidentales. Durante La Cumbre Mundial sobre la Sociedad de la Información (CMSI) celebrada en Túnez en 2005, ya se escenificaron los parámetros de ruptura. En primer lugar por el control real de los trece grandes nodos de la red (los que interpretan las DNS a nivel de nombres) controlados por EEUU de manera férrea[40], ubicados a lo largo de sus dos costas y comunicados con enlaces de fibra óptica submarina con el resto de nodos secundarios a lo largo de todos el territorio mundial[41]. En dicha cumbre EEUU y sus aliados consiguieron posponer el debate acerca de la

---

[38] Fidonet: http://www.fidonet.org/

[39] Fidonet España: http://www.fidospain.org/

[40] Matterland, A. *¿Hacia qué "Nuevo Orden Mundial de la Información"?.* En *Sociedad Mediatizada*. Gedisa. Barcelona, 2007.

[41] Distribución de los nodos servidores DNS raíz: http://norfipc.com/infografia/mapa-mundial-redes-conexion-internet.html

ICANN (Internet Corporation for Assigned Names and Numbers), que es la entidad privada que controla en última instancia la mayor parte de los nombres de dominios en la red. Como veremos más adelante, aunque entidades nacionales pudieron tomar el control de sus dominios, como el caso español con los dominios *.es* y su controvertida gestión a propósito de la acreditación de nombres y la posibilidad de enajenar dominios[42], las bases de la red siguen en manos estadounidenses.

[42] Estos dominos son gestionados por una entidad estatal, dependiente del ministerio de Industria, que verifica la posesión de nombres comerciales. Este tipo de gestión sirve como filtro para las identidaddes empresariales, aunque también ha supuesto su cuestionamineto por parte de privados, que pueden ver cómo su labor puede ser tomada si su web coinicide con el nombre de algún organismo oficial que exija su posesión: http://www.dominios.es/dominios/

1.4 Redes, Espías y Satélites

Efectivamente, se produjo un cambio respecto al paradigma de la seguridad, al socaire de una estabilidad relativa producto de una guerra fría que mantuvo durante varias décadas un estatus quo de "no agresión", entendida como despliegue directo y uso de todos los recursos disponibles, en el que se potenciara otras formas respecto a la inteligencia militar y una planificación de contingencias en caso de que finalmente se diera el peor horizonte de acontecimientos. De este modo, por un lado la denominada "inteligencia militar" comenzaría a recibir una financiación mayor por parte de las sucesivas administraciones norteamericanas, potenciando el avance técnico frente a la "clásica" red de informadores y espías de las agencias de información (CIA y NSA)[43] . Este interés y confianza en la aplicación de avances técnicos a la información militar llevaría incluso a grandes programas de reestructuración de dichas agencias, adelgazando la posición de su personal efectivo respecto a la inversión tecnológica, sobre todo desde la administración Reagan, que, como veremos más adelante[44], ha tenido consecuencias en la incapacidad de establecer seguimientos alguno de ciertas células terroristas en tiempos recientes. Bajo esa óptica, nacería ARPA (Advanced Research Projects Agency) en los 60', como respuesta a la amenaza potencial que la tecnología deducible del lanzamiento del *sputnik* significaba. Con el fin de establecer un sistema de comunicaciones resistente a un eventual ataque nuclear, Paul Baran, diseñaría, en Rand Corporation, durante los años 1960-64, un sistema de conmutación de paquetes (grupos de información fragmentada y codificada digitalmente) independiente de ningún centro de mando o control, de

---

[43] Armand Matterart .*Historia de la sociedad de la información*. Paidos: Barcelona. 2007

[44] . Breve diagrama sobre las primeras redes http://www.computerhistory.org/internet_history/

manera que cada unidad concreta pudiese encontrar la ruta de forma autónoma para el envío y recepción de mensajes[45].

Curiosamente, podemos hacer un seguimiento casi paralelo al de las diferentes administraciones, norteamericanas en su mayoría, y las formas que han ido tomando los diversos programas de control y comunicación militar. De este modo, las transferencias de fondos y el interés concreto han funcionado a impulsos bien definidos, sobre todo a través de contratas y programas diversos con un itinerario, la mayor parte de los casos, abocado al abandono, aunque con unas aplicaciones concretas que han posibilitado desarrollos independientes más que fructíferos, paralelo a los diferentes momentos, desde la "guerra fría", hasta la "lucha contra el terrorismo", la *Netwar* y la persecución de *hactivistas.*

La red *Echelon*[46] [47] será uno de los casos concretos en los que el espionaje tecnológico ha seguido el camino de los tiempos y los diversos focos de interés de los gobiernos liderados por el norteamericano y seguidos por aliados concretos, no todos ellos poseedores de toda la información que estas redes captan[48]. En 1948, con un hermetismo casi absoluto, hasta el grado de desconocerse la situación de muchas de las antenas en uso, surgía esta red, promovida por EEUU y cuatro aliados anglófonos (Canadá, Gran Bretaña, Australia y Nueva Zelanda). En esencia, Echelon es un sistema de escuchas global de todas las comunicaciones, cuyo caudal de datos es procesado por la NSA (agencia

---

[45] Mapas de la distribución de ARPANET por años
http://som.csudh.edu/cis/lpress/history/arpamaps/

[46] Recopilación de informaciones sobre Echelon en castellano
http://www.seprin.com/echelon.htm

[47] Otra compilación de datos sobre Echelon
http://www.sindominio.net/metabolik/alephandria/txt/faq_echelon.htm

[48] VV.AA Echelon. La red de espionaje planetario. Melusina. Barcelona. 2007

Nacional de Seguridad estadounidense), una intervención a escala mundial de todos los datos emitidos en llamadas telefónicas, faxes o correos electrónicos que emplea aparte de su propia red militar, satélites civiles con absoluta impunidad, caso del INTELSAT. Es, en definitiva, la concreción de las teorizaciones de la *Global Information Dominace.* De cualquier forma, lo que en principio fuera una forma de vigilancia militar, del enemigo soviético, pronto devendría en espionaje, inteligencia económica y fiscalización mundial; el caso reciente más conocido fue el del fracaso de las negociaciones de Airbus con el Gobierno Saudí a causa de unas informaciones que finalmente favorecieron a una contrata de Boeing[49] , esto llevaría en el año 2001 al parlamento europeo a realizar un informe llamado "Capacidades de Intercepción 2000"(23-*adjunto*), momento a partir del cual han ido surgiendo informaciones detalladas sobre el proyecto . ONG como Greenpeace también han denunciado estar entre sus objetivos, lo que demuestra cómo el itinerario de la captación de información ha ido derivando desde el fin de la guerra fría hacia otros fines[50] .

Ya desde 1965, el pentágono había llevado adelante la iniciativa de satélites de comunicación, en aquel entonces bajo el contexto de la guerra fría, orientado a "todo el mundo libre" denominado INTELSAT (International Telecomunications Satellite Consortium), que pronto pasaría a un uso masivamente civil, bajo la tutela norteamericana, adalid del comercio y la comunicación. En 1996, el pentágono crearía otra agencia de control, la National Imaginery and Mapping Agency, responsables, entre otros programas del conocido GPS (Global Positionig System) dedicado en principio a la dirección de misiles y posicionamiento de tropas y que

[49] Sobre el caso Airbus: http://news.bbc.co.uk/2/hi/europe/820758.stm

[50] Informe del parlamento europeo sobre Echelon: http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_es.pdf

posteriormente sería liberado para usos civiles, con señal degradada e intervenida en ciertos lugares, como forma de competir con el proyecto europeo Galileo, sistema de detección terrestre civil. En conjunción con la *US Air Force*, un nuevo programa de cobertura espacial denominado Future Imagery Achitecture, compuesta de veinticuatro satélites espías, con una precisión de quince centímetros, supondrá el programa de espionaje más caro de la historia.

El mundo a partir del 11-S

A partir de la *USA Patriot Act*, llevada adelante por la administración Bush tras el 11-S y su nuevo ministerio, El *Homeland Security Deparment*, llevará adelante un sistema de espionaje autorizado y reconocido como nunca antes, centralizado en la TIA (Total Information Awareness), un banco de datos integral, de todos los individuos, en los que se compilan todos los datos posibles de carácter personal, inscripciones y registros varios, datos bancarios, transacciones, suscripciones personales etc[51] .
A día de hoy, aún no ha sido derogada ni la ley, ni cambiadas las agencias concretas dedicadas a dichos fines. Otros Países, como es el caso de china, con su Ghostnet[52], ya cuentan con sus agencias de intervención informática, aunque de estos casos conocemos aún menos informaciones

[51] Armand Matterart .*Historia de la sociedad de la información*. Paidos: Barcelona. 2007

[52] Un artículo muy interesante al respecto, publicado por el diario The New York Times:http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1&pagewanted=2&partner=rss&emc=rss%3Cbr%20%3E%3C/a%3E

sobre su funcionamiento y tan solo nos llegan rastros de sus intervenciones concretas[53].

Curiosamente, la sección 215[54] de la Patriot Act ha expirado en junio de 2015[55] y la administración Obama ha establecido ciertos límites formales al control ciudadano extensivo por parte de la NSA, aunque en paralelo, ha mantenido resquicios legales para justificar su acción, lo que por la vía de los hechos supone un rechazo formal al espionaje pero un mantenimiento real de la vigilancia en la red de cualquier sujeto susceptible de ser incorporado como sospechoso, en un sentido muy amplio. Legislaciones como CISPA (Cyber Intelligence Sharing and Protection Act)[56], suponen un reconocimiento de que las agencias de inteligencia, especialmente los denominados centros de fusión contraterrorista, no sirvieron para su función formal [57] sino que han significado una conculcación de derechos privados sin resultado real que lo justifique[58]. Las sospechas se dispararían cuando el foco de buena parte de la atención de estas se revelara como dirigido al espionaje industrial y

---

[53] Padilla, M. *El kit de la lucha en internet*. Traficantes de sueños ed. Madrid. 2012

[54] La EFF hizo un exaustivo seguimiento de la Patriot Act y su uso concreto: https://www.eff.org/es/issues/patriot-act

[55] Sobre la "caducidad" de la sección 215: https://www.eff.org/es/deeplinks/2015/01/section-215-patriot-act-expires-june-congress-ready

[56] Sobre CISPA: http://www.eldiario.es/turing/aprobacion-CISPA-legalizara-espionaje-ciudadano_0_122837866.html

[57] El uso poco adecuado de los centros de fusión de datos desataría la polémica en la prensa estadounidense: http://www.wired.com/2012/10/fusion-centers/

[58] Las peticiones cívicas para el cierre de estos centros será una campaña destacada de colectivos cívicos en EEUU a lo largo de 2012: https://www.eff.org/deeplinks/2012/10/new-senate-report-confirms-government-counterterrorism-centers-dont-stop

gubernamental. La revelación del sistema PRISM[59], significará un punto de inflexión para este periodo de expansión del espionaje que ni siquiera la lucha contra la "ciberyihad", pudo contrarrestar suficientemente.

Como fuimos sabiendo por sucesivas revelaciones de WikiLeaks y posteriormente de E. Sowden (*véase 4.2 WikiLeaks, Whistleblowers, y grandes filtraciones)* El espionaje gubernamental ha sido una constante que permea todas las comunicaciones a escala global. No será hasta que se desate el escándalo hasta que se ha sabido el alcance real de todo el sistema creado por los EEUU. No obstante, otros estados también han elaborado sus programas de espionaje propios, como el SITEL español, puesto en marcha en 2007[60].

Pero no solo serán los estados los que se dedicarán a lo largo de este periodo de nuestra historia reciente a espiar y recabar datos de ciudadanos sino que grandes empresas han puesto el foco en el potencial de adquirir datos personales y procesarlos. El conocido como Big data, ha supuesto un salto en la calidad del procesado de información personal de personas a una escala no conocida a lo largo de la historia de la humanidad. En este sentido, poder filtrar y catalogar preferencias personales se ha convertido en una parte esencial para el foco publicitario, del que viven buena parte de los grandes de Internet. Casos como los de Facebook o Google[61], recurrentemente enfrentados a

---

[59] Las revelaciones de E. Snowden sobre el espionaje masivo significará un punto de inflexión cuyas consecuencias todavía no han desarrollado todo su alcance: http://andradesfran.com/prism-el-escandalo-de-espionaje-ciudadano-masivo/

[60] Publicacion en el Boletión Oficial del Estado del sistema SITEL: http://www.boe.es/buscar/doc.php?id=BOE-B-2007-256021

[61] Al respecto, escribiría varios artículos en su momento, que abundan en el tema de la vigilancia cuidadana “paralegal”: El avance de una videovigilancia y el análisis biométrico sin garantías

la Comisión y el parlamento europeo al entrar en conflicto con las legislaciones nacionales y comunitarias sobre la protección de datos personales, no hacen más que apuntar la dirección que se está tomando en la catalogación ciudadana y el su seguimiento[62]. Todo esto no ha sido posible sin una expansión de los medios de comunicación masivos hasta una escala global en la que, mientras se posibilita el acceso a una información constante[63], se asiste a una sobresaturación de esta hasta la conversión del ciudadano en consumidor[64]; en espectador pasivo que no pasa del *clicktivismo*[65] .

Una formula ya conocida como la de Mohaw Valley [66] o el "método científico para romper huelgas" que pasa por la transferencia de estados de opinión hacia conceptos vacíos de contenido real, a modo de eslogan generalista. Un trabajo de "ingeniería de consenso", en palabras de Chomsky, capaz del encubrimiento del objetivo real por la vía de la disgregación de la opinión y la fabricación de consensos artificiales. Así, "*bajo un aparente sosiego, todo indica, por contra, el esfuerzo del control social de este conjunto de recursos materiales y sociales de que dispone la sociedad para asegurarse la conformidad del comportamiento de sus*

---

ciudadanas: http://www.rebelion.org/noticia.php?id=170707

[62] Sin extender demasiado el tema, la pérdida paulatina del anonimato en nuestra sociedad es ya un hecho: Tu cara no es anónima http://andradesfran.com/tu-cara-no-es-anonima/

[63] Castells, M. *La era de la información: economía, sociedad y cultura (Vol. 3): .Fin del milenio*. Alianza editorial. Madrid. 2008

[64] Chomsky, Noam. *El control de los medios de comunicación*. Icaria. Barcelona. 2008.

[65] Una de las primeras referencias al clicktivismo en castellano la encotramos en el Blog de Enrique Dans: http://www.enriquedans.com/2014/02/clicktivismo-disenando-respuestas-en-un-panorama-diferente.html

[66] op cit.64

miembros en un conjunto de reglas" que "en efecto, están instalando nuevos métodos de coacción más sutiles, más insidiosos y eficaces".

Así podemos ver como la expansión de las comunicaciones ha sido desde sus comienzos empapada de medios de espionaje y control, en primer lugar desde los propios gobiernos y seguidamente desde el mundo de la gran empresa y que a la larga han establecido ciertas confluencias de intereses en detrimento de unas democracias cada vez más vaciadas de contenido. Como veremos, las posteriores revelaciones acerca de los nuevos sistemas de espionaje global con los que arranca el nuevo siglo, especialmente a partir de la segunda década, donde grandes filtraciones podrán al descubierto la sofisticación y el alcance de la vigilancia global, nos ubicarán en un contexto aún mayor de intervención estatal.

1.5 Ciencia, Universidades e Información

Continuado con los precursores de la red como existe hoy en día, la primera red de ordenadores, ARPANET[67], iniciaría su andadura en 1969, con la ubicación de sus primeros cuatro nodos en la Universidad de California en Los Ángeles, El Standfor Research Institute, La Universidad de California en Santa Bárbara y la Universidad de Utah. Esta red, estaba abierta a los miembros colaboradores con el Departamento de Defensa y pronto comenzarían a usarse para fines propios por parte de los científicos del proyecto, creando incluso una red de mensajes para aficionados a la ciencia ficción [68], rasgo singular que heredarían futuras redes: la imposibilidad de diferenciar entre comunicaciones militares, científicas y personales. En 1983, esta situación levaría a la escisión entre ARPANET, dedicada ya a fines científicos, y MILNET, exclusivamente dedicada a asuntos militares.

La Nacional Science Foundation, también comenzaría a desarrollar en los años ochenta otra red científica, CSNET y, en cooperación con IBM, otra red de disciplinas no científicas, denominada BITNET. A pesar de esa variabilidad, todas las redes usaban el *backbone* (red troncal de interconexiones) de ARPANET, y todavía a lo largo de toda esa década la red de redes sería denominada ARPANET-INTERNET y mantenida aun, en su estructura fundamental, por el Departamento de Defensa y gestionado por la National Science Foundation, que la mantendría operativa hasta febrero de 1990, momento en que esta última lanzaría de forma autónoma

---

[67] Sobre la gestación de ARPANET: http://www.nsf.gov/news/special_reports/nsf-net/textonly/60s.jsp

[68] . Manuel Castells. *La era de la información: economía, sociedad y cultura (Vol. 1): La sociedad red*. Alianza editorial. Madrid. 2008

el proyecto NSFNET (National Science Foundations Network) y MILNET comenzaría a funcionar por separado. Sin embargo, NSFNET solo estaría operativa como red durante cinco años, tras los cuales, bajo a presión de diversas entidades privadas, que mantenían sus redes, y otras no lucrativas para integrarse todas ellas en una gran red descentralizada con las características básicas de lo que hoy conocemos como Internet, a partir de diferentes proveedores de servicios (ISP) que conectan entre sí a los nodos de interconexión a las diversas redes y servicios integrados. Esto dejaría a la red de redes sin ningún tipo de dirección centralizada, lo que en ciertos aspectos podría suponer un problema, por ejemplo a la hora de establecer cómo se establecen los nombres y direcciones concretas a los que dirigirse, después de la creación de los protocolos OSI, para la estandarización, mediante diversas capas y niveles, de las formas de interconexión.

La primera infraestructura internacional de la red

En enero de 1992, la Nacional Science Foundation tomaría la iniciativa al impulsar la Internet Society, fundación sin ánimo de lucro que agruparía a las organizaciones coordinadoras que se habían gestado hasta el momento, la Internet Activity Board y la Internet Engineering Task Force, para principalmente coordinar a nivel internacional la asignación de dominios de Internet, asunto muy polémico que aún sigue dividiendo a las naciones hasta el punto crítico de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), de noviembre de 2005, celebrado precisamente en Túnez(país que no destaca por la apertura de sus redes o el acceso

libre a la información)[69], donde se abrió la posibilidad de volver a disgregarse.

En 1998, la creación de la ICCAN/IANA (Internet Corporation for Assigned Names and Numbers)[70], pretendía resolver los problemas en la asignación de nombres y direcciones. Sin embargo, su gestión no deja de ser polémica hoy en día, solo hay que observar su vertiginoso calendario de reuniones[71], sobre todo porque, a pesar de ser una fundación sin ánimo de lucro dedicada a organizar y gestionar una serie de nodos, no deja de ser a todas luces tendenciosa tanto su gestión como la distribución de estos. De hecho, la ICANN está constituida como una sociedad de derecho, radicada en California, por tanto bajo su jurisdicción legal y en última instancia, dependiente del Departamento de Comercio de EEUU. Su base de datos está controlada por otra entidad denominada VeriSign[72], otra empresa californiana que gestiona certificados y accesos seguros y validados a diversas webs de comunicación cifrada (la mayor parte de las https de bancos y otras empresas).

Los trece nodos centrales de ICANN, controlados por servidores denominados "servidores raíces", están instalados en Estados Unidos (cuatro en California y seis cerca de Washington), en Europa (Estocolmo y Londres) y en Japón (Tokio). EEUU hasta el momento, se ha cerrado al

---

[69] *Armand Matterart .Historia de la sociedad de la información. Paidos: Barcelona. 2007*

[70] Para saber más sobre la organización de ICANN.: http://www.icann.org/tr/spanish.html

[71] Los calendarios de ICANN han tenido un orden ascendente desde su creación, dadas las resistencias y conflictos que se han manifestado en su seno: 5. http://www.icann.org/en/general/calendar/

[72] La empresa VeriSign es uno de los puntos críticos de la red comercial: http://www.verisign.es /

debate sobre la apertura que reclaman otros países, bajo el argumentario de la defensa frente a ataques terroristas, impedir la censura o no caer en la burocracia[73] . Hasta el momento actual, todas las tentativas de crear un foro sobre el gobierno de Internet han caído en prácticas dilatorias y declaraciones de intenciones vacías de contenidos.

Definiendo las bases de comunicación

Los protocolos que usara en sus comienzos ARPANET, pasaban por conexiones de 56.000 bits por segundo. En 1987, la mejora en infraestructuras físicas lograba alcanzar los 1,5 millones de bits por segundo y la NSFNET funcionaba en 1992 a 45 millones de bits/seg., capacidad suficiente para posibilitar el envío de 5000 páginas por segundo. Sin embargo, el principal cuello de botella se encontraba en la capacidad de los diversos ordenadores de poder intercomunicarse entre sí, en un lenguaje común, adaptado al envío y recepción de paquetes decodificables. En 1973, Víctor Cerf y Robert Kahn, científicos informáticos que investigaban en ARPA, diseñarían los que llegaría a ser la futura infraestructura de Internet, basándose en los trabajos iniciados por el segundo en su empresa de investigación, la BBN. Con tal fin, convocarían una reunión en Standford a la que asistieron investigadores del ARPA, diversas universidades y centros de investigación, entre los que destacaba el PARC/Xerox, donde los trabajos de otro destacado científico, Robert Metcalfe acabará por conformar el protocolo de las actuales redes de área local (LAN).

[73] . Ramonet, I. *El control de Internet. En Le Monde Diplomatique*, 04/11/05

La cooperación que se puso en marcha incluía, asimismo, otros centros europeos, entre los que destacaban los franceses del grupo Cyclades. Sobre las bases de este seminario, Cef, Metcalfe y Gerard Lelann (de Cyclades) conformarían las especificaciones del protocolo TCP (Protocolo de Control de Transmisión), ajustado a los requisitos descritos por los diferentes investigadores del seminario y las características de las redes existentes en ese momento. En 1978, Cerf, Postel (de la UCLA) y Cohen, continúan desarrollando este concepto nuevo de puerto, como mecanismo de transmisión diferenciada de información entre ordenadores, dividiendo el protocolo en dos segmentos, que a partir de ese momento serían llamados TCP/IP (Protocolo de Control de Transmisión/ Protocolo de Internet), dedicado por una parte al ordenador principal, denominado *Host* y la otra al ordenador final con su intérprete. Este sufriría aun una serie de modificaciones para ajustarse de forma casi universal a las redes y conexiones posibles hasta estabilizarse en la versión TCP/IP v4, estándar de comunicación desde entonces, al asumir dentro de este el estándar europeo x.25, que amenazaba con ser un formato diferente y no compatible. De hecho, su flexibilidad y la capacidad de crecer y ser escalado sin problema, llevaría pronto a la migración completa de ARPANET en enero de 1983 a este protocolo, siguiendo la estela de los que había hecho en Departamento de Defensa de los Estados Unidos al declarar al protocolo TCP/IP el estándar para las comunicaciones entre redes militares, en marzo de 1982.

Todas estas acciones, acelerarán la convergencia tecnológica, al lograr estándares comunes sobre los que todos pudieran basarse a la hora de establecer comunicaciones o diseñar y emplear diversas aplicaciones en red, siendo el soporte efectivo aun de muchas de las aplicaciones más

populares de Internet[74]. Todavía una adaptación final del sistema operativo UNIX, creado por los laboratorios Bell en 1969 y base casi universal de la informática del momento, sería necesaria. Esta, financiada de nuevo por ARPA, y llevada a cabo por desarrolladores de la universidad de Berkley, se llevaría a término en 1983 y se distribuiría a precio de distribución, al haberse elaborado con fondos públicos.

La confluencia de medios que encontramos hoy en día en la red parte en buena medida de dichas especificaciones de base. Recientemente el protocolo HTML5 ha sido rediseñado para adaptarse a las nuevas tecnologías convergentes, entre las que destacan la integración de vídeo o la aceleración integrada en el navegador. El *W3 Consortium*[75], es la organización encargada de fijar los parámetros básicos de dicho lenguaje de programación que es de hecho el estándar web a día de hoy. La definición de estos parámetros no ha dejado al margen la polémica, al permitir la inclusión de DRM (gestión de bloqueos de derechos de autor) dentro de dicho código, aunque tales detalles se explicaran más adelante, adelantamos que esta visión favorable a los grandes negocios en la red constituirá parte del problema y las resistencias que mas adelante se desarrollen.

---

[74] Especificaciones del protocolo TCP/IP: http://www.rfc-es.org/rfc/rfc0793-es.txt

[75] . Estándar HTML5, del w3 consortium, trata de ser la base de desarrollo de la web actual: http://www.w3.org/TR/html5/

1.6 Hackers e investigación independiente

El debate sobre la definición de Hacker, en su traslado al castellano no está exento de polémica. La propia definición de este en el diccionario de la RAE[76] es tan confuso como falto de apego a una realidad concreta que es actualidad hoy en día y forma parte del propio origen y desarrollo de Internet. La definición tendenciosa que los asimila a "piratas informáticos"[77] algo bien alejado de una realidad en la que los expertos en seguridad informática, que deben tener amplios conocimientos técnicos y del arsenal de hacking para realizar su labor. Asociarlos a prácticas oscuras revela una falta de adecuación a una realidad que no es nueva. La reacción a este caso puntual por parte de la comunidad hispana, llevó incluso a una campaña en *Change.org*[78] para que se modificara esa definición[79], obteniendo la colaboración de personajes tan renombraados como Richard Stallman[80].

---

[76] La confusa y poco adeacuada denfinicion de hakcer que podemos encotrar en el RAE como “Pirata Informatico”: http://www.rae.es/

[77] la definición de hacker en la RAE. http://lema.rae.es/dpd/srv/search?key=hacker

[78] Petición en internet para que se cambie la definición de hacker: https://www.change.org/p/real-academia-de-la-lengua-espa%C3%B1ola-que-cambien-la-definici%C3%B3n-de-hacker-como-pirata-inform%C3%A1tico

[79] La polémica con la definición de Hacker. http://www.europapress.es/portaltic/portalgeek/noticia-definicion-hacker-rae-provoca-fuerte-polemica-20141027161250.html

[80] . Respuesta de Richard Stallman a la RAE: http://www.elmundo.es/tecnologia/2014/10/27/544dea28ca474156028b456b.html

Los expertos en seguridad deben conocer los instrumentos de análisis y explotación de redes e infraestructuras[81]. Con ello, reconocen un conocimiento avanzado de técnicas de hacking que al igual que otros instrumentos o herramientas pueden ser utilizados con muchos fines y que por ello no significa que estén diseñados para el empleo por parte de "malhechores". El Hacking ético, es la manera en la que se define la búsqueda de conocimiento y la exploración de debilidades y fallos, no para ser explotados sino para poner en conocimiento y mejorar los sistemas. La definición en habla anglosajona atina mucho más al definir tres tipos de actividad Hacker [82] : La White Hat (sombrero blanco), que bajo ningún concepto hace uso de los conocimientos y descubrimientos que adquiere durante su actividad; una definición en la que suelen encajar los, peritos informáticos, *Pentesters* (especialistas en la búsqueda de vulnerabilidades de sistemas) y profesionales de la seguridad en general. Los Black Hat son el punto contrario, que buscan y explotan fallos para poner en peligro sistemas, tareas de espionaje, robos de identidad y cometer delitos en general. El punto intermedio es el denominado Grey Hat, muy vinculado al denominado "hactivismo" (activismo que hace uso de herramientas de hacking). Casos como los ataques a ciertas compañías, organizaciones y gobiernos por parte de comunidades de usuarios y grupos bajo el nombre de Anonymous, Lulzsec y otros, muchos de ellos surgidos a raíz de comunidades de usuarios como 4Chan[83], son ejemplo de ello.

---

[81] . González Pérez, P. *Ethical Hacking*.0xWorld, Madrid. 2014

[82] Himanen, P. *La ética del hacker y el espíritu de la era de la información.* Destino. Barcelona. 2004

[83] 4Chan es el foro anónimo que dio origen al termino *Anonymous*, dado que todos sus usuarios se muestran con tal nombre si no escriben voluntariamente otro y por tanto posibilitó un grado de libertad absoluto a la hora de propagar memes y acciones: http://www.4chan.org/

Entre sus acciones son típicos los ataques DDoS (denegación de servicio mediante el bombardeo de peticiones a un servidor hasta su saturación) o la suplantación y cambio de contenido de ciertas páginas a modo de protesta.

La definición del afamado creador de una de las páginas más reputadas de habla inglesa BoingBoing y escritor Cory Doctorow[84], es muy acertada al hablar de "pioneros digitales" que buscan el conocimiento por encima de restricciones poco ajustadas a la realidad. Lo cierto es que esta subcultura, surgida alrededor de unas técnicas, ha adquirido un peso considerable en la creación de Internet y su intervención es uno de los pilares que ha condicionado la forma en la que sistemas y redes se integran en la actualidad[85] . En más de una ocasión, nos encontraremos a lo largo de nuestro estudio con la reacción de la comunidad, cada vez más en sincronía con el activismo cívico, que ha comenzado a ser consciente del papel preponderante que las comunicaciones tienen en la defensa de derechos y libertades y el peligro real que existe de supresión de estas de forma no reconocida democráticamente por parte de unos estados cada vez más identificados con las prácticas lobistas que no deja de ser una forma sutil de definir legalmente la corrupción a gran escala[86] .

---

[84] Doctorow, C Little Brother. Disponible en http://craphound.com/littlebrother/download/

[85] Cory Doctorow*: "En veinte años todos nuestros problemas estarán relacionados con Internet*": http://www.eldiario.es/catalunya/Cory-Doctorow-problemas-relacionados-Internet_0_392661817.html

[86] Castells, M. *La era de la información: economía, sociedad y cultura (Vol. 3): .Fin del milenio*. Alianza editorial. Madrid. 2008

Uno de los principios de la cultura "Hacker", aceptando el término que la propia comunidad de expertos ha venido a bien adoptar, es la puesta en común de sus investigaciones, el sentido colectivo, en cierto modo emparentado con una ética libertaria. Dos de sus figuras claves Richard Stallman[87] y Linus Torvalds, creadores de GNU (lo que hoy se entiende de forma simplificada como Software Libre) y del núcleo del sistema operativo Linux, respectivamente, han sido desde el principio claves en la difusión de esta óptica. En concreto Stallman, ha jugado un papel preponderante en la extensión de códigos abiertos en la programación, confrontando con el software privativo y comercial, cerrado e imposible, por tanto de ser mejorado y evaluado por la comunidad de informáticos, es decir, se trata de lo contrapuesto a una programación transparente y de libre acceso. El debate es bien extenso y abarca lo que explicaremos en sucesivos capítulos a propósito de derechos de autoría, propiedad intelectual y el papel de las patentes y el concepto de "propiedad" en la era de la información[88].

El hacking como investigación y mejora de las formas de comunicarse en la red

A partir de la puesta en marcha de los medios para comunicarse y extender una red abierta y extensa de dispositivos informáticos , se produciría una interconexión a gran escala de redes y centros diversos,

---

[87] Stallman, R. *Software Libre para una sociedad libre*. Traficantes de sueños Ed. Madrid. 2013. Edición electrónica: http://www.traficantes.net/libros/software-libre-para-una-sociedad-libre

[88] . Stallman, R. y otros. *Contra el Copyright*. Tumbona Ediciones. México. 2008. Edición electrónica: http://bibliotecalibre.org/handle/001/352

acelerando aún más el proceso de convergencia de aplicaciones y aunando investigaciones entre equipos cada vez más remotos. De hecho, los propios científicos protagonistas de estas investigaciones serían los primeros en ir migrando entre diversos centros y creando un ambiente de colaboración general en el que el flujo de ideas y cocimientos era una constante. Sin embargo, como hemos adelantado más arriba, junto con el pilar científico y militar, básicos a la hora de sentar la estructura fundamental de la red, se encuentra el de los propios usuarios o hackers, término que ha sufrido una curiosa deriva desde sus orígenes, como definición de la excelencia en el conocimiento, a una interpretación menos benigna que no deja de ser en muchos casos tendenciosa, que aportarían grandes innovaciones a esta red recién creadas. De hecho, esta nueva red en auge de principios de los ochenta no sería la misma sin la aportación y las implementaciones de usuarios desinteresados. Uno de los casos singulares más destacados sería el del correo electrónico, cuyo uso, a pesar de experimentos anteriores de escritura sobre servidores en tiempo compartido, forma primigenia de mantener e intercambiar informaciones direccionales, sería introducido por Ray Tomlinson, que buscaba una forma más directa de envío de información entre ordenadores contra destinatarios concretos y no sobre directorios de acceso compartido. Para tal fin, desarrollaría un par de aplicaciones de envío y recepción de mensajes. También empleó la arroba (@) para separar el nombre del usuario del servidor que aloja el programa de recepción de correo, eligiendo este carácter por ser el único término ausente de todos los apellidos y nombres. En poco tiempo, el correo electrónico pasaría a ser la aplicación más empleada en Internet, llegando a ser una de las formas de comunicación actuales más empleadas y de mayor implantación, paralela a la propia red[89] .

[89] Cronología de las comunicaciones y precursores del correo electrónico: http://www.telecable.es/personales/carlosmg1/historia_correo.htm

Otro gran fruto de esta nueva contracultura de la red, los hackers, sería la invención del módem. En 1978, dos estudiantes de Chicago, Ward Christensen y Randy Suess, idearon la forma de enviarse y transferir información desde sus ordenadores personales domésticos durante el frío inverno de esta zona estadounidense, mediante un sistema que usara la línea de teléfono para acceder a las redes a las que en aquel momento solo algunas instituciones estaban conectadas. De hecho, el término módem (*Mo*dular/*Des*modular), proviene de su función codificadora de datos a través de pulsos pasados a digital a través de una línea analógica y el proceso inverso por parte de la unidad receptora. En 1979, habían desarrollado el protocolo *Módem*, que permitía a los ordenadores la conexión y transferencia de archivos sin pasar por ningún servidor central y, lo que aún será más importante, difundirían el código fuente y las especificaciones de forma gratuita, lo que significaría la gran expansión de esta tecnología entre los ordenadores que hasta el momento se encontraban excluidos de las grandes redes corporativas o institucionales. Al poco, tres estudiantes de la Duke University y de la Universidad de Carolina del Norte, ambas no incluidas aun en ARPANET, crearían una versión modificada de los protocolos del sistema operativo UNIX para conectar ordenadores entre sí, empleando la red telefónica convencional.

A partir de estas posibilidades de conexión universalizada, entre los poseedores de la tecnología y los conocimientos, se crearía un foro de discusión en línea (*on line*- a través de la red) sobre temas informáticos en principio denominado *Usenet*, primer sistema de comunicación entre internautas a gran escala. Los inventores del Usenet News, también

permitirían el uso libre de su código, distribuido en una conferencia sobre Unix.

Aprovechando el potencial de las BBS (Bulletin Board System - *Sistema de tablón de anuncios)* ya preexistentes, aunque integradas, en principio, en el sistema de las grandes redes dependiente de un servidor centralizado, Tom Jennings diseñaría en 1983, un sistema para envío de boletines de anuncios a través de Internet empelando un software específico diseñado para aprovechar el potencial del mecanismo de los módems. Esta nueva interfaz, daría origen a una de las redes más populares a lo largo de toda la década, *Fidonet*[90], ya que integraba las posibilidades de estas BBS de forma automática, simplificando el proceso de acceso. Al ser una red barata y abierta, se convertiría en una de las más populares, agrupando en 1990, 2.500 ordenadores solo en EEUU, y extendiéndose por todo el mundo[91], hasta que, el surgimiento de la World Wide Web (la red de hoy en día), mucho más dotada tecnológicamente, la fuera desplazando.

Las primeras grandes comunidades virtuales surgirían al calor de estas aplicaciones concretas, desarrolladas por los propios usuarios, al margen o paralelamente a las investigaciones militares o académicas y puestas en común, en la mayor parte de los casos, en toda la colectividad.

---

[90] 15. Fidonet http://www.fidonet.org/

[91] 16. Fidonet España http://www.fidospain.org/

Estas redes, al margen de la Internet *general*, llegarían a suponer en su conjunto, al calor del progresivo abaratamiento de costes y la cada vez mayor integración de ordenadores en el ámbito académico, que inducía la adquisición de uno personal a los estudiantes, la red mayoritaria en cuanto a terminales y personas conectadas. A pesar de este éxito inicial, progresivamente irían decayendo en favor de servicios conectados directamente en la red global y como sucede de manera recurrente en los servicios más populares, terminarían en desuso.

Como hemos visto, ya desde sus orígenes el mundo y la ética hacker han formado parte sustancial de la gestación de las primeras formas de red que se formaran desde antes de la gran expansión de Internet. Una de las tesis principales del presente trabajo será rastrear la importancia no reconocida que la capacidad de trabajo de comunidades de desarrolladores y activistas ha tenido en la manera en la que conocemos hoy en día Internet. La implementación de diferentes bloques no siempre unívocos es lo que hoy en día configura esta red.

1.7 La Gran Red Mundial- World Wide Web

El nivel de penetración en la red de la población mundial [92] especialmente en estados de corte occidental[93] ha conseguido hoy en día unos niveles que hacen pensar en una sociedad cada vez más conectada. Internet está llegando a todas partes[94]. y no es un fenómeno nuevo, aunque su extensión crece de forma exponencial ya no se puede afirmar que sea un proceso para valorar como hecho periodístico sino que forma parte de los últimos tiempos de nuestra historia reciente[95]. El mundo actual no se puede comprender sin el impacto de las redes y estas tampoco sin saber cuáles han sido los agentes que han intervenido en su configuración[96] .

Continuando con el hilo de los cambios y las entidades y personas que iniciaron el agregado de recursos y especificaciones que componen hoy la red mundial llegamos al momento en el que se define

---

[92] . UIT (ITU) datos sobre la penetración de Internet en el mundo en el periodo 2000-2015 https://www.itu.int/net/pressoffice/press_releases/2015/17-es.aspx

[93] Gráficas de acceso a Internet en Europa: http://epp.eurostat.ec.europa.eu/tgm/mapToolClosed.do?tab=map&init=1&plugin=1&language=en&pcode=tsiir040&toolbox=legend

[94] . Augé, M. *Sobremodernidad: del mundo tecnológico de hoy al desafío esencial del mañana*. En Sociedad Mediatizada. Gedisa. Barcelona.2007.

[95] Internet world stats. Estadísticas mundiales sobre Internet: http://www.internetworldstats.com/

[96] Página de la CIA sobre acceso a internet y otras tablas estadísticas: https://www.cia.gov/library/publications/the-world-factbook/rankorder/2153rank.html

finalmente. Hasta este momento, hemos visto como se había establecido los niveles de enlace entre máquinas pero la proliferación de redes alternativas, con su diversidad de protocolos y normas de acceso, aisladas de hecho entre sí, hacía que hasta el momento no resultara del todo fácil, para el profano en temas informáticos, llegar a conectarse o integrarse desde casa a una de esas redes, que también arrastraban ciertas limitaciones en cuanto a la cantidad de datos transmisibles o la capacidad de transmitir lo que no fuera texto plano. Así, las redes que se habían configurado hasta el momento no habían podido dar el salto al usuario doméstico o la pequeña empresa.

El siguiente salto tecnológico se daría en Europa, en el CERN (*Conseil Européen pour la Recherche Nucléaire- Consejo Europeo para la Investigación Nuclear*) [97] . Efectivamente, con la tentativa de poder gestionar mejor la información disponible mediante una interfaz informática y basándose en los conocimientos preexistentes sobre el hipertexto, Tim Berners-Lee y Robert Cailliau, ambos investigadores del centro, diseñarían el HTML (HyperText Markup Language -Lenguaje de Marcas de Hipertexto), conjunto de instrucciones para el diseño accesible de documentación. Asimismo, diseñarían el primer *Navegador* (intérprete de estos hipertextos), con la idea de diseñar un formato de libre disposición de la información de manera horizontal. En su diseño, se habían inspirado más en los diseños autónomos de las redes informales que en los oficiales de ARPANET, lo que era posible dado que el HTML formateaba el documento a partir de los protocolos TCP/IP, independientemente de la máquina en cuestión. Para poder interpretar estos documentos alojados en diversos servidores o repositorios, colaborarían también en el estándar HTTP

[97] 6.El CERN ha sido uno de los nodos inciales de la investigación y extensión de la red de redes: http://public.web.cern.ch/public/

(*HyperText Transfer Protocol*- Protocolo de Transferencia de Hipertexto)[98]

En conjunción a todo lo anterior, para saber direccionar la ubicación de los documentos y resolver su dirección específica, crearían un formato estandarizado de resolución de direcciones denominado URL (Uniform Resource Locator- Localizador Uniforme de recursos), a través del cual poder encaminar las peticiones de documentos HTML concretos, ofreciendo en un conjunto el protocolo y la ubicación concreta del recurso deseado. Con todo ello, crearían la *World Wide Web* (Gran Red Mundial), dado que, al ser por un lado la forma más simple y capacitada de resolución y gestión de protocolos y ser un estándar abierto, que el CERN distribuiría libremente a través de Internet, pasaría a ser la base de todo Internet futuro, al que las otras redes pronto se sumarían para convertirse en el primer formato de intercomunicación informático mundial. El primer servidor Web sería puesto en línea el 6 de agosto de 1991. Para aquel entonces, el CERN era ya el principal servidor de contenidos de Europa, con una catalogación por temas y no por dispositivos físicos donde se ubican realmente dichas informaciones, dotado, por tanto de un sistema más eficaz de consulta y una forma por primera vez "virtual" de gestionar estos. Los primeros *sites (*sitios o servidores de contenido) comenzarían inmediatamente a incorporar esos protocolos y formatos para mantener su información, sobre todo los grandes centros de investigación científica.

Las bases de la red mundial ya estaban fijadas, establecidas bajo unos principios de código abierto, al margen de estándares patentados o propietarios y por tanto con la posibilidad de ser modificados o investigados abiertamente para poder implementar cualquier mejora. Precisamente esta

[98] Especificaciones del HTTP del W3 consortium http://www.w3.org/Protocols/

motivación, sería la que impulsara a un joven becario de la NCSA (National Center for Supercomputer Aplications), Marc Andreessen, a buscar una forma de explorar la red mediante una interfaz gráfica, que empleara el ratón ,en lugar del modo texto, empleando la consola con una serie de comandos prefijados como se accedía hasta entonces[99]. Con este fin, crearía Mosaic, el primer gran navegador con capacidades gráficas, que sería distribuido gratuitamente a través de la página de la NCSA desde noviembre de 1993, convirtiéndose de forma rápida en el navegador principal de toda la comunidad y contribuyendo, por su facilidad de uso respecto a los formatos anteriores, en uno de los grandes difusores de la *World Wide Web*. Justo después de su graduación, en 1994, Jim Clark, otro de los nombres claves en la producción de software libre y dueño por aquel entonces de Sillicon Grafics (una de las compañías claves en la elaboración de sistemas de modelado gráfico para ordenadores), le propondría crear una nueva empresa que denominarían Netscape Communications Inc. *Netscape* sería su producto estrella y durante mucho tiempo prácticamente el navegador que monopolizaría el 90% de los ordenadores que accedían a Internet. A partir de esto, la historia de este navegador en bien conocida por el público y una de las primeras grandes causas contra Microsoft[100]. Efectivamente, esta compañía reconocería pronto el posible potencial que los navegadores y las redes en general tenían en el futuro de la informática y en una de esas historias truculentas que tanto han caracterizado a muchas de estas empresas, y a Microsoft especialmente, se harían con el código fuente de Mosaic, para adquirir su licencia y elaborar en un desarrollo propio, denominado Internet Explorer, que incorporaría a su sistema operativo hasta terminar por copar el

[99] Manuel Castells. *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*. Plaza & Janes. Barcelona. 2001

[100] Castells, M. *Innovación, libertad y poder en la era de la información. En Sociedad Mediatizada*. Gedisa. Barcelona, 2007.

mercado anterior de Netscape, que finalmente, una vez desalojado del mercado en la práctica, sería vendido al proveedor de contenidos AOL[101]. Con los años, el código liberado de éste pasaría a una fundación creada alrededor de un nuevo proyecto denominado Mozilla, cuyo producto estrella será el navegador Firefox.

El caso antimonopolio de Microsoft (el primero de ellos) será seguido con gran interés por la prensa mundial y empresas del sector. La apuesta de Microsoft fue la de erradicar la competencia mientras hacía una potente campaña de imagen por parte de su fundador y CEO, Bill Gates, entre la que destaca la creación de la fundación *Bill y Melinda Gates*, que destina cantidades millonarias a diferentes proyectos benéficos. En el segundo Bloque del presente trabajo trataremos sobre los diversos frentes legales de la compañía y el papel de esta y otras grandes de la primera fase de expansión de la red en situaciones de monopolio[102].

---

[101] Ramonet, Ignacio. Pensamiento único y nuevos amos del mundo. Icaria. Barcelona. 2008

[102] Dans, E. Todo va a cambiar. Deusto. Madrid. 2010
El profesor E. Dans en su libro Todo va a cambiar. Hace un extenso análisis de Microsoft y su posición dominante. En su capítulo 10 disponible en http://www.todovaacambiar.com/capitulo-10-un-caso-practico-microsoft

1.8 Sistemas operativos y Red

El último pilar para que la informática personal se popularizara y estos nuevos estándares de redes, ya fijados a principios de los noventa, se pudieran extender entre un público que transcendiera el ámbito académico o ligazón a usuarios de informática relativamente expertos sería el de los sistemas operativos y el subsiguiente software sobre el que hacer uso de las nuevas máquinas y sus accesos. Como ya resumiéramos antes, Unix era un sistema realmente caro para usuarios finales y estaba quedando circunscrito al ámbito académico y empresarial, mientras que los sistemas operativos de Apple mantenían una restricción en cuanto a que solo era posible hacerlos funcionar en su hardware propietario, ligando este a la propia máquina en la que corre. El terreno estaba quedando por tanto, expedito para el mercado de las máquinas clónicas corriendo sobre un sistema operativo que pronto se demostraría de facilidad de uso similar al Mac (Apple Macintosh) y lo que es más importante aún para su difusión definitiva, de fácil copia para los usuarios finales[103]. De hecho, es a partir de esa práctica de universalización de copias del ordenador de IBM y de copias (en muchos casos) del sistema operativo de Microsoft, en sus diversas versiones para usuarios finales, todas ellas sobre la base de MS-DOS, es decir su sistema de consola, a la que se superponían las sucesivas versiones de Windows, con su capa de modo gráfico GUI (Graphic User

---

103

1. Gráficos sobre la evolución de microprocesadores

- http://www.network-press.org/?que_es_microprocesador
- http://www.intel.com/products/processor_number/chart/
- http://www.youtube.com/watch?v=trBZXWIX8Zk&feature=related

Interface) que, traída como remedo de la de Apple, sería la base definitiva de su popularidad [104] . Una de las claves del éxito del modelo *Wintel* (Sistema operativo Windows sobre procesadores Intel o compatibles) ha residido tanto en el abaratamiento de la una producción deslocalizada, con preeminencia de China, como en la capacidad de distribución del software de forma no controlada[105].

Para servidores y empresas continuaría usándose sistemas propietarios de red, sobre todo basados en la robusta arquitectura de UNIX y sus derivaciones (como Sun Solaris en Bases de datos), donde las versiones profesionales de Windows (NT, 2000, 2003 o 2008) mantendrán cuotas de mercado más reducidas, a pesar de la estrategia de la compañía desde principio, los grandes servidores corporativos irán progresivamente apostando por alternativas de software libre (GNU)[106], especialmente entre algunas que ofrecen soporte profesional como Reh Hat o Suse Linux.

---

[104] Metzner-Szigeth, A.*: "El movimiento y la matriz" – Internet y transformación socio-cultural.* En: Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación (CTS+I), No. 7, 2006

[105] Castells, M. *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad.* Plaza & Janes. Barcelona. 2001

[106] GNU, sobre las categorías de código abierto existentes: http://www.gnu.org/philosophy/categories.es.html#CopyleftedSoftware

El beneficio comercial de la llamada piratería de Software

Efectivamente, las copias "piratas" (sin licencia) del sistema operativo de Microsoft, así como de su paquete de software ofimático "*office*", que en principio fuera marginal frente a alternativas como *WordPerfect* o *StarOffice*, conseguirían copar el mercado de este tipo de máquinas a precios muy reducidos respecto a la competencia[107]. Aunque no declarada, siempre ha existido una posición ambigua al respecto[108]. Si bien es cierto que el objetivo de la compañía en diversas campañas contra las copias no licenciadas de sus aplicaciones y Sistemas operativos estaban orientadas a la gran empresa y la administración pública, con diversos y recurrentes acuerdos con estas últimas para la implantación de sus servicios, no existió un sistema de control de copias para usuarios domésticos, más allá de ciertas notificaciones en las versiones más recientes muy fáciles de remover y popularmente muy extendidas. De hecho, la estrategia OEM, incluyendo en equipos nuevos una versión del Sistema Operativo vinculada exclusivamente a estos, se ofrecía dentro del precio para grandes distribuidores que en la mayor parte de las ocasiones continuaban ofreciendo el producto al cliente final con la opción de venta sin sistema operativo, lo que nos confirma que no se trazó una estrategia contra el usuario doméstico. Una vez acostumbrado en un ámbito al uso de un software, el usuario medio resulta acomodaticio, por lo que busca tener el mismo software en todas las máquinas que emplea. Los descuentos del paquete Office para estudiantes, abundan en esta óptica: Acostumbrar a un

---

[107] La polémica sobre si beneficia la piratería a Microsoft ha sido ampliamente discutida y documentada en la red:http://www.enriquedans.com/2007/03/microsoft-y-la-pirateria.html

[108] El ejecutivo de Microsoft, Jeff Raikes, aseguraría en 2007 que la piratería es buena para la compañía.http://www.informationweek.com/if-youre-going-to-steal-software-steal-from-us-microsoft-exec/d/d-id/1052865?cid=rssfeed_iwk_all

uso para que luego, en la empresa, resulte complejo tratar de instalar alternativas. Aún hoy en día, tras el desarrollo de paquetes de código abierto (Open Source) Como OpenOffice [109] o el más reciente *LibreOffice*[110], que de hecho son en la práctica iguales al paquete de Microsoft, la mayor parte de la comunidad de usuarios sigue optando por emplear versiones no licenciadas de este último.

Dicha laxitud, vino acrecentada por la nueva tendencia hacia el empleo de equipos portátiles, en donde comenzaría a disputarse el terreno de nuevo, sobre todo por los equipos de Apple en el mercado de estadounidense. Contra esa tendencia hacía una marca, los fabricantes optarían por recuperar la anterior estrategia de equipos a menor coste frente a los iDevices (equipos de la marca Apple) que cuentan con un precio que le permite a la compañía unos mayores márgenes.

Para un productor de software cualquiera y especialmente para Microsoft, tan vinculado a los fabricantes de equipos, sobre todo cuando enfrente tiene un entorno cerrado de equipo y software, como es todo el ecosistema creado por Apple, en el que sistema operativo, navegador, paquete ofimático e incluso herramientas de edición avanzada de fotografía y vídeo, son ofrecidas de una vez con la compra del equipo, lo que significa en la práctica una barrera muy compleja para introducir sus productos, la estrategia debe adaptarse a los nuevos tiempos.

---

[109] Open Office surgiría bajo el auspicio de Oracle como como desarrollo libre en contraste con los paquetes ofimáticos de microsoft: https://www.openoffice.org/es/

[110] Tras una ardua polémica por parte de los desarrollladores de Open Office con Oracle, que pretendía mantener cierto tipo de control sobre un producto esencialmente libre, la mayor parte de los desarrolladores implicados en el poryecto migrarían a uno nuevo denominado LibreOffice:. https://es.libreoffice.org/

Que la estrategia de la compañía cambia de enfoque lo confirma el propio Satya Nadella[111], CEO de Microsoft, desde 2014, cuando apunta que la compañía siempre ha ofrecido el modelo *Fremium* (modelo gratuito con limitaciones) gracias a la piratería. Una situación que ya era un lugar común entre consejos de administración de la compañía, como revelara en 2007 uno de sus directivos. La constante ha sido en este sentido la anulación de la competencia mediante prácticas monopolistas[112] o de adquisición de innovaciones antes de que se extiendan[113]. El mercado de adquisiciones de las grandes de Internet, como se verá más adelante, se ha convertido en un agregado en el que casi no quedan resquicios para el negocio independiente, más allá de la expectativa de entrar en el mercado de adquisiciones tras un lanzamiento sin modelo real de negocio, como han sido los casos de *YouTube, Skype* o *WhatsApp* por nombrar los más destacados.

Internet se hace móvil

Por otro lado, Apple también abre un frente nuevo en la navegación, adelantándose a los nuevos tiempos en los que la movilidad y la versatilidad

---

[111] Entrevista al actual CEO de Microsoft, Satya Nadela, donde afirma que su modelo gratuito ha sido siempre la copia pirata: http://www.cnbc.com/id/102101929#

[112] Sobre la competencia desleal de Microsoft se ha documentado ampliamente por muchos especialistas del sector: http://eparalosnegocios.blogspot.com.es/2010/10/caso-microsoft.html

[113] Primera sentencia, de 2002, contra Microsoft: http://www.justice.gov/atr/cases/f200400/200457.htm

entre diversos equipos junto con una capacidad de acceso cada vez mayor a la red imponen nuevas pautas de navegación. La aparición del iPhone, en esencia una evolución estéticamente mejorada del *PocketPC*, que propiciaba Microsoft junto con Intel y de las anteriores Palm, y más adelante el iPad, una tableta que depuraba la idea del UMPC (Ultra Mobile PC) entre otras, dejaba a las marcas tradicionales, muy vinculadas a las pautas de Microsoft, totalmente fuera de mercado. De nuevo grandes empresas del sector móvil, verán como sus sistemas operativos, excesivamente rígidos y controlados, entran en crisis como el caso de Symbian, perteneciente a Nokia, que será definitivamente abandonado y lastrará las ventas del líder del sector del momento hasta la práctica insignificancia y su final adquisición, precisamente por Microsoft. Las agendas electrónicas de *Palm* y su sistema operativo PalmOs, llevaban activos desde 1996 y tenían cierto impacto en entornes empresariales. Más adelante *Blackberry*, retomaría la idea integrándola con una movilidad incipiente. Aun así, todos estos entornos ofrecían un escaso atractivo por diversos motivos para convertirse en un dispositivo convergente, en el que, aparatos portátiles para audición de música (incluso vídeo), telefonía, comunicación, agenda y ocio en general pudieran presentarse en un único dispositivo de bolsillo. Los tímidos intentos de los Pocket Pc, chocarían con la barrera de un sistema operativo no suficientemente cuidado por parte de Microsoft, demasiado cerrado y que no avanzaba al ritmo de las comunidades de desarrolladores que al encontrarse con un software privativo, ofrecían muchas de sus soluciones como *hacks* (a modo de truco no oficial) de sistema o versiones *underground*, fuera del reconocimiento legal y por tanto muy minoritarias.

Como vemos, ninguna innovación resultaría sustancial pero si la presentación y el momento de unir todas ellas en una solución convergente. Tras el intento fallido de un teléfono capaz de emplear iTunes (la plataforma de sincronización de contenidos de Apple), en colaboración con Motorola en 2005, se insistió en un dispositivo

convergente totalmente controlado por la compañía. La presentación del iPhone en enero de 2007, tendrá un gran impacto entre un sector tecnológico que como hemos apuntado no estaba avanzando lo suficiente respecto a las posibilidades que podía ofrecer un producto de estas características. La creación de una necesidad de consumo, junto con una presentación del producto impecable, proyectaron los niveles de ventas del dispositivo a cifras no alcanzadas por otros dispositivos con conexión a Internet. La capacidad de soportar aplicaciones desarrolladas por terceros, tras su pertinente aprobación y la comisión de ventas por parte de la compañía de la manzana, así como una producción masiva en colaboración con diferentes factorías de ensamblado ubicadas en China, no exentas de polémicas como las reveladas por las condiciones de trabajo de las fábricas de FoxConn[114], crearían una hegemonía en el mercado de dispositivos inteligentes a la que no se respondería de forma adecuada hasta al menos un par de años después, con la tercera versión del sistema operativo móvil basado en Linux desarrollado por Google.

Efectivamente, no sería hasta que otra de las grandes compañías de Internet, Google, ofreciera a fabricantes la posibilidad de realizar dispositivos móviles con un sistema operativo de código abierto (aunque desarrollado en sus respectivas versiones por Google) que de nuevo aparecería una alternativa real a los productos propuestos por Apple. Auspiciado por la *Open Handset Alliance*[115], una fundación que agrupa a varias compañías tecnológicas, lideradas de forma indiscutible por Google, en pos de estándares abiertos para dispositivos móviles, el sistema operativo Android será la tabla de salvación de una serie de compañías que

---

[114] Extenso reportaje de The New York Times sobre las consecuencias en coste humano del modelo de producción del iPhone y el iPad por parte de Apple: http://www.nytimes.com/2012/01/26/business/ieconomy-apples-ipad-and-the-human-costs-for-workers-in-china.html?_r=2&pagewanted=all

[115] La *Open Handset Alliance:* http://www.openhandsetalliance.com/

habían quedado fuera de mercado tras la implantación de iOs. La apuesta temprana de empresas como HTC, que lanzaría el primer dispositivo con este sistema operativo, el *HTC Dream*, o Samsung será la clave para plantear una alternativa clara al sistema de Apple. Tal es así que la reacción de esta compañía, arrastrada por el obcecamiento de su CEO, Steve Jobs, embarcará a Apple en una ofensiva jurídica por infracción de patentes que llegaría a límites esperpénticos, como el registro del uso de pantallas táctiles[116]. De hecho, la *guerra de patentes* desatada llevaría a varias compañías al registro de patentes cada vez más absurdas o de difícil defensa (como se verá en el bloque III del presente trabajo). Como curiosidad, en 2012 Samsung fabricaba más de un 60% de los componentes de los primeros iPhone, algunos de ellos tan esenciales como la propia pantalla o el procesador.

Como conclusión a este apartado, podemos señalar como la red de redes surge como un proceso en el que convergen agentes diferentes que no encajan con la imagen de mito fundacional que ciertamente es traída en múltiples ocasiones de jóvenes estudiantes que triunfan desde su garaje. El Internet actual es la confluencia del interés militar, primero producto de la guerra fría y que luego derivara a conceptos de "seguridad" y "lucha contra el terrorismo", el interés científico por investigar e implementar aplicaciones y el de agentes individuales y colectivos, en muchas ocasiones hackers y activistas del software libre, con objetivos diversos pero que dotaron a la red de su dimensión social colectiva y abierta que hoy conocemos.

---

[116] El caso Apple vs samsung: https://www.evernote.com/shard/s43/nl/4889222/f5c04aec-1031-4385-8bb6-03ea4304be0f/?csrfBusterToken=U%3D4a9a86%3AP%3D%2F%3AE%3D14e0651055e%3AS%3Dc59cb45da5629c0ee1d22b602c62d462

En palabras de Manuel Castells: *"Fueron los hackers, generalmente universitarios, quienes desarrollaron Internet como red de comunicación informática global. Y fue la comunidad internauta la que se autogestionó, de forma diversa, a lo largo del tiempo, desde 1969, primer despliegue de Internet, hasta la constitución de ICANN en 2000. No hizo falta ni derecho de propiedad ni control burocrático para desarrollar la red de comunicación más potente de la historia. En realidad, fue la no existencia de esos controles lo que lo hizo posible"*[117]. Sería efectivamente esta falta de controles, o la intencional imposibilidad de control, que no de vigilancia una de las características que hacen de la red de Internet uno de los medios de comunicación más libre que existe, dado que todas las comunicaciones pueden realizarse de forma completamente desintermediada. Esto no excluye que se esté dando una auténtica "guerra por el dominio de los recursos multimedia", en palabras de Ignacio Ramonet[118]. Una guerra no siempre sutil, a través de cuyas aristas podemos deducir la profundidad de los cambios que implican y su incidencia social, como veremos en el siguiente capítulo.

---

[117] 3. Manuel Castells. *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*. Plaza & Janes. Barcelona. 2001

[118] 16. Ramonet, Ignacio. *Pensamiento único y nuevos amos del mundo*. Icaria. Barcelona. 2008

II : Organización de la red y su papel en la "Nueva Economía";

2.1 Actores y agentes

Como apuntábamos en el bloque anterior, la red de redes, como la conocemos, es producto de una tensión permanente entre dos tendencias contrapuestas: Por un lado, el intento permanente de control y dirección por parte de ciertos gobiernos y empresas del sector, y por otro la absoluta libertad, apertura y organización en forma de agregado caótico de los diversos elementos protocolos y servicios que la integran. El cuadro no quedaría completo sin la delimitación de los tres agentes citados. Si bien puede ser cierto que ciertos gobiernos se han identificado plenamente con gigantes del sector con un interés estratégico, sobre todo en el caso de Estados Unidos y de mantenimiento de una hegemonía heredada desde el inicio del tendido de la infraestructura que soporta al sistema hasta hoy en día, también hay que mencionar casos en los que la propia justicia y legislativos como el la Comisión Europea han actuado limitando el alcance de ciertas tecnologías[119]. Entre los casos reseñables podemos destacar la retirada de la tecnología de etiquetado y reconocimiento facial por parte de Facebook en Europa [120] [121], aunque el caso conlleva sus propias connotaciones respecto a quien debe vigilar a la ciudadanía y quien gestiona los datos[122], o el del "derecho al olvido" que afecta especialmente

---

[119] . *Respecto al caso de reconocimiento facial de Facebook, han sido varias las polémicas consecutivas. La compañía ha tratado en varias ocasiones de implantar dicho sistema, primero probando con el consentimiento de usuario, cambiado sus políticas de privacidad y por último buscando acuerdos con diferentes instancias gubernamentales.* https://nakedsecurity.sophos.com/es/2012/09/23/under-pressure-facebook-disables-facial-recognition-in-europe/

[120] La polémica sobre esta retirada del reconocimento facial tendría repercusión mundial: https://www.eff.org/deeplinks/2012/07/eff-asks-supreme-court-reverse-forced-consent-facebook-decision

[121] . Facebook lo intentó en varias ocasiones en Europa. He seguido personalmente el caso en varios artículos como el que sigue: http://www.eldiario.es/turing/Facebook-comenzara-perfil-reconocimiento-facial_0_170083259.html

[122] Sobre el caso, el que escribe también recogería informaciones detalladas sobre las

al buscador de Google[123]. La explicación del primero de estos agentes ya nos ofrece la narración del segundo y su contexto. La gran empresa enfocada a Internet, ha sido capaz de una expansión como nunca antes había logrado empresas de un sector "emergente". Los denominados " *Grandes de Internet*"[124], cuyo negocio principal o buena parte de este está vinculado directamente a servicios ofrecidos o vendidos a través de la red, consiguen manejar un conjunto de recursos financieros tales que se encuentran en posición de adquirir anualmente tanto compañías que arrancan en el sector como atacar a sectores menos directamente vinculados a su negocio como conglomerados mediáticos y editoriales[125] o productoras culturales. Con ello, se colocan en el centro de difusión de la cultura global[126] con un escaso contrapeso por parte de las democracias y la ciudadanía. El tercer agente y sujeto capaz de establecer influencia y condicionar su parte de la mutación que la red vive como parte de esta dinámica de contrapuestos es la propia ciudadanía, sus partes más concienciadas y los individuos capaces de establecer parámetros de cambio. No solo se trata de activismo o hactivismo, como se ha definido a la actividad legalmente límite con la que se encauza una contestación

---

formas de obtención y manejo “paralegal” de datos biométricos: http://andradesfran.com/tu-cara-no-es-anonima/

[123] En otra colaboración con elDiario.es también tratarái sobre la recolección de datos: http://www.eldiario.es/turing/vigilancia_y_privacidad/videovigilancia-analisis-biometrico-garantias-ciudadanas_0_149435381.html

[124] Sobre los "grandes de internet" frente a la vieja empresa: http://www.genbeta.com/activismo-online/la-guerra-de-los-gigantes-de-internet-la-prensa-escrita-y-el-viejo-conglomerado-mediatico

[125] 7. Chomsky, Noam. *El control de los medios de comunicación*. Icaria. Barcelona. 2008

[126] 8. Echeverría, J.: Los Señores del aire: Telépolis y el Tercer Entorno. Barcelona (Destino) 1999

organizada. Las nuevas capacidades de organización y difusión de contenidos, ahora no ya tan limitadas por la propiedad de los medios entre sujetos activos, ha propiciado el establecimiento de redes contestatarias ciudadanas que emergen en situaciones concretas. Ejemplo paradigmático es la paralización de ACTA[127], el acuerdo multilateral contra la piratería [128], que supuestamente actuaba en defensa de la propiedad intelectual, pero que en cuyo texto real trataba de extender la censura y vigilancia en la red a escala global, entregada a agentes no electos. Precisamente será la filtración de su contenido lo que impida que gobiernos de países de Latinoamérica y Europa puedan asumir el costo de lo revelado hasta el momento y finalmente acabe con el abandono del proyecto[129].

Sociedad de la información e ideología dominante

A la sociedad de la información en la concepción difundida, se corresponde una ideología implícita del pensamiento único [130], forma

---

[127] La negociación de ACTA sería una de las grandes legislaciones capaces de agrupar una contestación global de organizaciones cívicas de origen diverso: http://www.stopacta.info/

[128] La Quadrature du net, será uno de los medios digitales que mas detalladamente nos ofrecerá información sobre el estado de los diversos acuerdos de carácter similar a ACTA: https://wiki.laquadrature.net/How_to_act_against_ACTA

[129] . Los sucesivos intentos de aplicar acuerdos supranacionales para favorecer intereses poco declarados han sido extensamente tratados a lo largo de la presente década en diversos medios. El tema en cuestión lo he tratado de forma resumida en artículos como el que sigue, que en sí mismo enlaza de forma sumaria a los elementos más destacados: http://www.eldiario.es/turing/inocencia-red-internet_0_146635468.html

[130] 12. Ramonet, Ignacio. *Pensamiento único y nuevos amos del mundo*. Icaria. Barcelona. 2008

concreta del neoliberalismo económico, que bajo la terminología de una globalización unívoca[131] trata de imponer una serie de patrones y normas como formas derivadas del progreso tecnológico, asociando ideas y conceptos interesadamente, de manera que solo un análisis superficial, carente de crítica, sería capaz de no encontrar contradictorio. En este escenario, la tecnología y la gran expansión que la nueva cultura de la red global trae consigo son uno de los agentes principales del cambio social. Este será el elemento más atractivo de control y dirección de una sociedad, en palabras de Brzezinski, "cuya forma viene dada en el plano cultural, psicológico, social y económico por la influencia de la tecnología, más concretamente, la informática y las comunicaciones"[132].

La asociación de posmodernidad y sociedad de la información es, desde este punto de vista, casi una vía automática. La coincidencia de la explosión y la penetración en la sociedad de las nuevas tecnologías y formas de comunicarse, o recibir información, se ha dado en un momento de auténtica debilidad entre los agentes de movilización social, la crisis ideológica, la carencia de referentes culturales y la falta de teorizaciones sobre un modelo social, al margen de la tentativa de formateo intencional que el mundo de la empresa privada, en busca siempre de beneficios inmediatos por encima de cualquier otro objetivo, propaga desde el aluvión de información que propaga y controla[133] . Como veremos más adelante, ya no solo se trata de una parrilla televisiva puesta al servicio de unos intereses y un modelo social "*hegemónico*",entendido en términos

---

131 Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

132 Brzezinski, Z. *La Era tecnotrónica*. Paidós, Buenos Aires, 1979

133 Rebillard Franck. *De OhmyNews a Meidapart: ¿un nuevo modelo de periodismo*? ; En El estado de Mundo 2009. Akal. Barcelona. 2008

gramscianos[134], sino de una dirección completa, a través de grandes conglomerados mediáticos cuyas identidades políticas se circunscriben a familias de intereses, a modo de conjuntos, pero cuyos patrones apenas difieren en matices, a veces necesarios para marcar diferencia aparente más que auténticamente a partir de una reflexión o teorización concreta[135].

Este será uno de los conflictos recientes más claros, al derivar la libertad de expresión, principio básico de nuestras sociedades defendido como uno de los pilares de las democracias de nuestro tiempo, en libertad de expresión *comercial* (Marcket mentality) en palabras de Matterland, al ser los únicos en poseer la capacidad de hacer llegar su mensaje, invadiendo todos los espacios públicos, confundiendo diversidad cultural con la multiplicidad de oferta comercial e identidad con afinidad a una marca [136] . Este mismo autor sostiene cómo sobre el paradigma *tecnoinformacional* pivota un proyecto geopolítico a gran escala, que no es otro que el del liberalismo clásico, remozado en su terminología con nuevos términos tecnológicos. Así asistimos a la implantación de una forma de ejercer el poder denominado "*soft powe*r" (poder blando) en el que el modelo democrático estadounidense y el libre mercado modelan la sociedad desde las fuentes de este nuevo poder, que pasan por el paulatino desmantelamiento del estado nación, pilar de las democracias occidentales, en pos de unas comunidades de consumidores vacías de contenido real y fundamentadas en un "modelo gerencial" de lo público, una

---

[134] 16. Gramsci, Antonio. *Cuadernos de la Cárcel*. Ediciones Era. México. 1981

[135] Bell, Daniel*. El Fin de las ideologías: sobre el agotamiento de las ideas políticas en los años 50*. MTyAS. Madrid. 1992.

[136] Matterland, A. *¿Hacia qué "Nuevo Orden Mundial de la Información"?*. En Sociedad Mediatizada. Gedisa. Barcelona, 2007.

"sociedad de peaje" privatizada[137]. La obsesión por la seguridad y el control será el otro pilar sobre el que se cimienta el modelo ideado y una de las claves para comprender las fuentes del conflicto social sobre el que basamos el presente trabajo.

Así, la excusa tecnológica y la expansión de los mercados de la "era global" ha sido la explicación oportuna para ejercer un poder desde unos centros de decisión reales fuera del ámbito político[138] y por tanto ajeno a la esfera del control democrático. Por otra parte, asistimos a una "auténtica guerra por el dominio de los recursos multimedia y de las autopistas de la información" [139]. La criminalización de los medios independientes de distribución culturales, precisamente en unos tiempos en los que la precarización laboral impediría cada vez en mayor medida el acceso a los medios con los cauces, en muchos casos obsoletos, de venta y disfrute será una de las líneas de fractura de este ejercicio de dominio cultural. El impulso al consumo mientras los cauces legalmente reconocidos para ello adolecen de una obsolescencia absoluta, terminara por fortalecer la idea de la gratuidad en la descarga de contenidos. Las diferentes etapas de este recorrido, comenzando con la música y terminando por el cine y la literatura, demuestra la recurrente falta de una visión adaptada por parte de los antiguos poseedores de estos medios, mientras que otras ideas más adecuadas al consumo en red se hacen hueco, como el de la venta de *eBooks* (libro electrónico) por parte

---

[137] Chomsky, Noam. *El control de los medios de comunicación*. Icaria. Barcelona. 2008

[138] 12. Ramonet, Ignacio. *Pensamiento único y nuevos amos del mundo*. Icaria. Barcelona. 2008

[139] 21. Ramonet, Ignacio. *El control de Internet*. En *Le Monde Diplomatique*, 04/11/05

de *Amazon* o la difusión de series y cine con *Netflix*, por poner ejemplos de referencia.

El ejercicio del poder durante las crisis, en el sentido clásico del análisis del sistema capitalista, son el medio de coacción perfecto para una sociedad perpleja, que ante una situación excepcional tolera sin cuestionamiento el avance de ideas arrogadas de una excepcionalidad no necesariamente enlazadas con la situación planteada y que ni siquiera son una solución real a esta. La doctrina de la Escuela de Chicago, buscará la situación excepcional en la guerra y el terror como el aderezo adecuado a la crisis económica, producto de la aplicación dogmática de su política económica, para poder ejercitar sin respuesta su ortodoxia doctrinal[140].

En resumen, el ejercicio de un poder económico fuera de control democrático y subalterno del gran conglomerado de los gigantes de la nueva economía[141] junto con la gestión interesada de la crisis, la criminalización desproporcionada del delito sobre la "propiedad intelectual" y la obsesión por la seguridad, devenida a vigilancia sistemática y global junto con la administración del terror, entendido como un permanente estado de *excepcionalidad* alimentado por un enemigo oportunamente recurrente, conforman los cuatro pilares fundamentales sobre los que se cimienta la sociedad de entresiglos y las bases sobre las que debemos analizar cómo se desarrolla Internet desde sus orígenes hasta nuestros días.

---

[140] 22. Kleim, N. *La doctrina del Shock. El auge del capitalismo del desastre*. Booket. Madrid. 2012

[141] 23. Ugarte de, D. *Los futuros que vienen*. Colección Biblioteca de las Indias. Madrid. 2010

Nuevo modelo de empresa, nueva respuesta y organización ciudadana

A lo largo de todo el presente bloque reconoceremos las pautas y agentes que han posibilitado la expansión de un nuevo modelo económico. O la forma remozada del modelo preexistente bajo unos patrones ajustados a un formato empresarial distinto a los modos acostumbrados de empresa y su capitalización bursátil, que irrumpiera con fuerza en última década del siglo pasada con los valores del NASDAQ de Nueva York como referencia internacional y que vino a denominarse "nueva economía". Como análisis subsiguiente a esta expansión empresarial deberemos rastrear su repercusión en los medios de comunicación tradicionales y la propia reconversión de estos a formas adaptadas a los diferentes modos de estas empresas. De este análisis, partiremos para analizar otros dos elementos, siguiendo la idea de Don Tapscott y Antony Willians, al hacer referencia a la obsolescencia actual de todas las reglas que han presidido la forma actual de organización del trabajo y como resultan contraproducentes para la sociedad actual dos grandes pilares de la empresa capitalista de la edad contemporánea: la jerarquía y la protección de la propiedad intelectual[142].

Efectivamente, en estos dos terrenos veremos como las respuestas han sido diferenciadas dependiendo de qué agentes, de los que describimos desde el comienzo como pioneros de internet, actúen en cada ocasión. Por un lado, tenemos el modelo de empresa distribuida, en los que la inmediatez y la horizontalidad, en cuanto a los niveles de mando, la dotan de mayor eficacia, pero que frente a la creatividad y la propiedad intelectual presentan una visión ambivalente, ya que mientras que algunas

[142] Mounier, Pierre. *Las nuevas tecnologías de la información y la crisis de la cultura*; en El estado de Mundo 2009. Akal. Barcelona. 2008

corporaciones ,caso Microsoft, pretende tutelar y mantener el monopolio de todo el proceso y la propiedad de los resultados a comercializar; otras, como Google, potencian la investigación libre de sus propios empleados y promocionan elementos de colaboración para sacar productos al mercado a los que adaptarse y mantener la ventaja competitiva de la que lucrarse[143].

En el otro extremo, los usuarios independientes, programadores y teóricos del software libre, promueven unas formas colaborativas de creación, sin ánimo de lucro, o posibilitando el negocio en la asistencia o soporte más que en la propiedad intelectual [144], con iniciativas que transcienden el terreno informático para extenderse, mediante el uso de licencias como las de *CopyLeft*[145] o *Creative Commons*[146], como ejemplos masc representativos a cualquier forma de difusión cultural. En este terreno, sobre todo en lo que a la música respecta, formas al margen de las legislaciones sobre la propiedad intelectual también han prosperado, bajo el estigma interesado de "piratería", como formas de compartir información, las más de las veces sin ánimo alguno de lucro por parte de los desarrolladores del software concreto. En este sentido resultaría interesante ver cómo aplicaciones que se han enfrentado a los tribunales han sido luego absorbidas y reconvertidas en negocio, como ha sido el caso de la pionera Napster[147]. Mientras tanto, otras redes y páginas de enlaces

---

[143] 25. Reischl, G. *El engaño de Google*. Medialive Content. Barcelona. 2008

[144] Tipos de licencias Libres : http://www.gnu.org/philosophy/categories.es.html#CopyleftedSoftware

[145] http://www.fundacioncopyleft.org/

[146] http://es.creativecommons.org/

[147] El Napster actual nada tiene en común con la iniciativo de 1999: http://free.napster.com/

desde Audiogalaxy a *The Pirate Bay*[148] han servido de base a toda una cultura *underground que* se ha gestado precisamente en respuesta, en muchos casos a él obcecado uso de licencias de software abusivas, en contraste con modelos de negocio abiertos en total consonancia con esta cultura, como podría ser el caso de *Spotify*[149], software que nos permite escuchar gratuitamente cualquier canción de forma completamente legal, permitiendo al usuario final elegir entre un modelo de suscripción con acceso completo o un modelo con ciertos límites en la gestión y uso, con publicidad pero que permite el acceso a toda la biblioteca de medios.

Tanto el modelo de empresa basado en el paradigma de las grandes corporaciones de Internet, de las que buena parte de su negocio inicial fuera la red o servicios y productos informáticos, como el modelo de hacktivista, sea desde el activismo legal, que lucha y se organiza por derechos ciudadanos y sobre todo contra las restricciones de los derechos de autoría, o desde una actitud activa que bordea la legalidad de diversos estados, no se circunscribe a modelos cerrados[150].

El debate permanente entre tendencias de los activistas de Internet no es ajeno al modo en el que estos se producen entre otros movimientos sociales de carácter democrático y tendencias posibilistas, como por ejemplo la inclusión de la posibilidad de visualizar contenidos con DRM (un sistema restrictivo de gestión con copyright) por parte de la Fundación Mozilla[151] en su producto estrella, el navegador Firefox, que

---

[148]EL mayor tracker de archivos Torrents y Magnet y referencia mudial sigue siendo The Pirate Bay: http://thepiratebay.org

[149] http://www.spotify.com/en/

[150] . Lessig.L. *Por una Cultura libre. Cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad*. LOM. Santiago, 2005. Edición electrónica: http://www.traficantes.net/libros/por-una-cultura-libre

[151] 33. Sobre la fundación Mozilla: https://www.mozilla.org/es-ES/mission/?icn=tabz

desataría una serie de furibundas respuestas a lo largo de 2014 entre asociaciones[152] y destacados miembros de la comunidad identificada con el Software Libre, como el caso de Cory Doctorow[153], que veían en ello una claudicación frente a una red restrictiva.

Por su parte, la gran empresa de Internet, jugará una posición ambivalente respecto a los gobiernos y las comunidades de usuarios. Tras el descalabro de Nokia, al negarse a liberar el código de su sistema operativo *Symbian* para que una comunidad de desarrolladores pudieran mejorarlo, Google tomaría nota y permitiría el desarrollo del sistema operativo Android, precisamente como respuesta al ecosistema de software cerrado de Apple, su gran competidor[154]. Lo cierto es que en origen, sus fuentes de negocio principales eran diferentes y a la gran G, lo que más parecía interesarle era que muchos dispositivos visualizaran la publicidad que integraba su sistema y por ello no había empacho alguno en liberar su código fuente[155]. Para comprender el alcance de su apuesta respecto al software libre tan solo tenemos que acudir a su respuesta ante bloqueadores de anuncios o el desarrollo de líneas paralelas de Android sin integrar las aplicaciones de Google como el caso de *CyanogenMod*[156], para

---

[152] Reacción de la Free Software Foundation ante la inclusión de DRM en Firefox: https://www.fsf.org/es/noticias/la-fsf-condena-la-colaboracion-entre-mozilla-y-adobe-para-apoyar-la-restriccion-digital-de-derechos-drm

[153] . La respuesta de Cory Doctorow a la inclusión de DRM en Firefox: http://www.theguardian.com/technology/2014/may/14/firefox-closed-source-drm-video-browser-cory-doctorow

[154] 25. Reischl, G. *El engaño de Google.* Medialive Content. Barcelona. 2008

[155] Un acercamiento a la disputa abierta en los dispostivos móviles podemos consultarla en: *Los dispositivos móviles y Android .Entre la libertad y el interés comercial*: http://www.rebelion.org/noticia.php?id=170590

[156] 38. CyanogenMod pararía de grupo interesdado en una Rom modificada, a fundación y finalemente a empresa que colabra con fabricantes de dispositivos móviles, especialmente de orgen Chino: http://www.cyanogenmod.org/

ubicar a estas empresas más allá de su imagen corporativa, ampliamente *trabajada*. Otro momento clave será el de las revelaciones a propósito del espionaje masivo de usuarios, principalmente por parte de Estados Unidos y sus aliados cercanos. La colaboración absoluta de estas compañías[157], en su mayor parte entidades de derecho radicadas en suelo estadounidense, no deja de situarnos en la línea de otra de las claves de nuestra investigación y nos permite ubicar perfectamente qué lugar ocupa cada uno de estos agentes más allá de sus declaraciones de intenciones.

[157] Sobre el escándalo PRISM, una de las primeras revelaciones de Edward Snowden: http://andradesfran.com/prism-el-escandalo-de-espionaje-ciudadano-masivo/

2.2 Internet y Nueva Economía

La denominada Nueva Economía, en términos estrictos, no se circunscribe a las empresas tecnológicas o ligadas a Internet propiamente, sino que describiría a todas las que por un lado integran las nuevas herramientas de gestión y por otro siguen el modelo empresarial de estas. De cualquier modo, se trata de un modelo que se está difundiendo rápidamente a escala mundial. No nos es ajeno que a pesar de los elementos individuales o colectivos que han desarrollado las bases de buena parte del Internet actual, la innovación tecnológica se ha dirigido esencialmente al mercado. Ninguna empresa o estado, ha buscado el desarrollo de la tecnología por si misma o para el aumento de la productividad en beneficio de la humanidad. Actúan inmersas en un contexto histórico concreto, que fija una serie de reglas, las del *Capitalismo Informacional*[158], en palabras de Castells. Serán la rentabilidad y el aumento del valor de sus acciones los principales factores que motivarán los movimientos de estas empresas. Las instituciones políticas, moldeadas en su mayor parte de un "pragmatismo neoliberal", base de la "sociedad de mercado", en la que el *soft power* (poder blando) convierten la información en una forma de poder[159] . En manos de la "ingeniería del consenso", capaz de aislar las opiniones incluso mayoritarias tras un aluvión de informaciones capaces de "crear" estados de opinión contrapuestos no solo al interés general sino incluso en función a intereses concretos que objetivamente no serían refrendados si fueran puestos bajo un análisis honesto y ajustado a la realidad.

---

[158] Manuel Castells. *La era de la información: economía, sociedad y cultura (Vol. 1): La sociedad red.* Alianza editorial. Madrid. 2008

[159] Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

La receta económica concreta con la que se dirige esta *nueva economía* es, por otra parte, todo un clásico del liberalismo: la reducción de los costes de producción, donde la mano de obra es siempre uno de los primeros elementos, sobre todo en un momento de escasa organización y respuesta, aumentar la productividad, ampliar el mercado y acelerar la rotación de capital. En este contexto, el nuevo paradigma tecnológico solamente supondrá un entorno diferente del de las sociedades industriales precedentes, muchos de cuyos elementos no han dejado de existir ante el advenimiento de las nuevas formas de organización empresarial , como veremos, aunque si son presa, bajo las nociones de mercado bursátil y financiero actual, de la voracidad de empresas con capitalizaciones de dimensión hasta hace poco insospechada, dado su a veces escaso vínculo con la "economía real"[160].

Si complicada es la supervivencia de modelos de producción donde la capitalización se realizaba con un objetivo concreto, menos halagüeña es la perspectiva del empleo en este nuevo paradigma. Incluso la nueva élite de trabajadores de las grandes corporaciones tecnológicas de red y mediáticas, están sujetos a la misma contradicción entre capital y trabajo, radicalmente acentuada ante la mejora, cada vez mayor, de la productividad del trabajo[161], completamente absorbida en beneficio de la empresa, bajo la tensión de la reconversión permanente, con empleos a corto plazo, de rápida rotación, que bajo la justificación de la competitividad toma los métodos de coacción empresarial entre un "mercado laboral", (concepto que asimila a la población trabajadora como mercancía) cada

---

160 Chomsky, Noam. *El control de los medios de comunicación*. Icaria. Barcelona. 2008

161 OIT. Informe sobre productividad del trabajo http://www.ilo.org/global/lang--es/index.htm

vez más alejado de asideros indentitarios, organización efectiva o capacidad de respuesta.

Mercados volátiles y productividad

Por otro lado, las reglas de la producción continua, del nuevo positivismo económico con su fe en el crecimiento constante, arrastra a la producción hacia una cultura de la novedad permanente [162], y la obsolescencia programada de la producción[163], que ya al salir al mercado tienen relevo previsto en los diseños de planificación empresarial. Todo ello bendecido desde el nuevo "*Pret a penser*"[164] del nuevo paradigma de la empresa-red descentralizada y autónoma, que opera casi de forma directa con el consumidor con el modelo B2C (B*ussines to consumer*), al que incluso las empresas automovilísticas se están adaptando, condicionando la estabilidad de las plantillas de las subcontratas de piezas específicas. Esta volatilidad, llevada a todas las escalas, está suponiendo un cambio en las relaciones laborales y el modelo empresarial traído desde la óptica concreta de la doctrina económica del neoliberalismo, en la que el peso bursátil de las empresas adquiere preponderancia sobre la producción concreta, llevando a las cifras de resultados a ser más fruto de entornos especulativos que ligados a la producción real. Una de las consecuencias de mayor calado en este sentido será el de las aceleradas fusiones y absorciones de empresas dentro del entorno bursátil sobre bases insospechadas, como el caso, antes citado, de la adquisición de Time-

---

[162] Martín-Barbero, J. *Tecnicidades, identidades, alteridades: desubicaciones y opacidades de la comunicación en el nuevo siglo*. Sociedad Mediatizada. Gedisa. Barcelona. 2007

[163] 6. Marcuse, H. *El hombre unidimensional*. Ariel. Barcelona. 1994

[164] 2. Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

Warner, uno de los grandes conglomerados mediáticos de EEUU y primero a escala mundial, por parte del proveedor de servicios de Internet AOL (América Online) con una capitalización bursátil sobredimensionada sobre la base de la gran burbuja de las empresas del NASDAQ (indicador bursátil de Nueva York sobre las empresas del sector tecnológico) de principios de este siglo, respecto a la capacidad efectiva de la segunda[165]. De este modo, empresas cuyo basamento está más fijado en la capitalización bursátil que sobre la economía productiva, comenzarán a destacar y medrar con empuje en esta nueva economía. Su paralelo en otros sectores será solo cuestión de tiempo.

Este proceso de fusiones-adquisiciones, por encima de la inversión o innovación efectiva, empujará pronto a un complejo proceso de uniones a gran escala, como la adquisición de NBC por parte de *Microsoft*, creando el conglomerado MSNBC, o la unión en Europa de *Viviendi*, *Universal* y *Canal+* (Francia en concreto).

De este modo, vemos como la "nueva economía", se sustenta sobre el entramado de una doctrina que impulsa la óptica de una sola forma de organización social posible, asociada a la ley del mercado y el proceso de globalización[166] y una tremenda candidez positivista en cuanto a la fe en el progreso tecnológico como *posibilitador* de cambios por sí mismo. Como veremos más adelante, el férreo control de los derechos de propiedad intelectual será la gran batalla de esta época, dado que su control, una vez fijadas las reglas del pensamiento único, en palabras de Ramonet, es la clave del control de la riqueza. Será por ello por lo que el

---

[165] Bustamante, E. *Hacia un nuevo sistema mundial de comunicación: las industrias culturales de la era digital*. Gedisa, Barcelona, 2004

[166] Castells, M. *Innovación, libertad y poder en la era de la información. En Sociedad Mediatizada.* Gedisa. Barcelona, 2007.

marco legal respecto a lo que se denomina piratería entrará en conflicto permanente con los movimientos de libertad, en un proceso de expropiación comercial de la cultura[167].

En lo que respecta al positivismo tecnológico, como motor y salida constante de la crisis mundial, tema casi recurrente en el sistema mundial actual[168] , podría analizarse en los términos que propone Wallernstein, como salida hacia adelante que pospone el proceso contradictorio de la propia estructura fundamental del sistema, cuya tensión entre direcciones opuestas socava su propio futuro. La expansión ilimitada parece ser el medio de recreación de la estructura de privilegio desigualitario, que siempre ha encajado hasta ahora con el esquema clásico de Kondratieff, lo que no quiere decir ni que este tenga carácter de regla ni que nos sirva de prospectiva futura sino más bien como forma de análisis de las circunstancias económicas de los periodos anteriores. Las sucesivas llamadas a los finales de ciclos críticos no tendrán bajo esta perspectiva mayor valor que el de expresiones de deseo o intentos de condicionar opiniones bajo una hegemonía política y mediática que silencia por la vía de los hechos cualquier expresión de alternativa.

---

[167] Matterland, A. *¿Hacia qué "Nuevo Orden Mundial de la Información*"?. En Sociedad Mediatizada. Gedisa. Barcelona, 2007.

[168] Wallernstein, I. *Geopolítica y Geocultura. Ensayos sobre el moderno sistema mundial*. Kairós, Barcelona, 2007

Una crisis dirigida

En este contexto, la profunda crisis económica con la que concluye la primera década del siglo no sirve para reorganizar un esquema doctrinario que ahondaba en ésta sin ofrecer una salida viable a las sociedades. Por contra, las recetas derivadas de los organismos responsables principales de la difusión de esta doctrina, Banco Mundial, Fondo Monetario Internacional y en el caso europeo la Comisión Europea o el Banco Central Europeo han aprovechado la crisis como excusa para acelerar el proceso de enajenación global de bienes, recursos y servicios. En palabras de Eduardo A. Vizer, "*la globalización, pretende la reconversión todas las sociedades nacionales (económica, política e institucional)". "Las fuerzas hegemónicas pretende instaurar un sistema mundial exclusivamente bajo la metáfora instrumental (lógica de la máquina y también lógica de la eficiencia económica)"*[169]. Así, la crisis económica ha servido a una élite empresarial que cada vez acumula más poder (en forma de *lobby* o de forma directa) para profundizar en el modelo social y económico de un neoliberalismo que no encuentra respuesta efectiva en el plano democrático. Armand Matterlart, lo explica de forma contundente al afirmar que " *el paradigma tecnoinformacional se ha convertido en el pivote de un proyecto geopolítico cuya función es garantizar la reordenación neoeconómica del planeta en torno a los valores de la democracia de mercado y en un mundo unipolar*"[170].

---

[169] Vicer, E. *Procesos socioéticos y mediatización en la cultura tecnológica*. En: VV.AA. Sociedad Mediatizada. Gedisa. Barcelona.2007

[170] 2. Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

La fuerza de irrupción del modelo, dejará a la ciudadanía, como trabajador individualizado y precarizado, en permanente reconversión y competencia, bajo la amenaza de la exclusión social, en un estado de perplejidad permanente. Todas las certezas que la democracia de corte occidental ofrecía, bajo el paradigma del estado del bienestar, han sido conculcadas de forma abrupta, bajo la excusa de la crisis. Un asalto completo a tres de los pilares básicos del entredicho "estado del bienestar", el empleo (precarizado), las libertades públicas (controladas) y el espacio cívico (privatizado)[171]. Se nos presenta un "futuro enfermo"[172] en el que las respuestas no son en ningún aspecto hegemónicas y lo más parecido a una extensión social global no puede ser una red como Facebook ni la "auidienciación" que ofrecen los medios de comunicación actuales, con usuarios muy activos pero limitados y circunscritos al esquema cerrado de la tecnología ofrecida. El proceso de reconstrucción de identidades resulta algo segmentado pero no es patrimonio de *fundamentalismos* ni nacionalismos trasnochados, también existe un ámbito global de respuesta que comienza a tomar conciencia de su peso, que se informa al margen de los medios tradicionales y comienza a organizarse mediante redes de base.

Los tiempos históricos no beben de la inmediatez acelerada en la que está sumida nuestra sociedad. La organización de un contrapoder surge de forma paulatina, en forma de agregación de nodos locales y luchas concretas. La resistencia al pensamiento único, al poder unívoco, viene tanto por parte de colectivos clásico, activismos, sindicatos,

---

[171] Kleim, N. *La doctrina del Shock. El auge del capitalismo del desastre*. Booket. Madrid. 2012

[172] 15... Ugarte de, D. *El poder de las redes*. Colección Biblioteca de las Indias. Madrid. 2011

organizaciones políticas alternativas al sistema, como por parte de formas nuevas que convergen en un proceso en el que la participación es la clave. A lo largo de los años 90 del pasado siglo, movimientos como el Foro social Mundial, ATTAC o el encuentro mundial de organizaciones frente al neoliberalismo, auspiciado por la guerrilla pacífica del EZLN, formaron las bases de una red internacional de respuesta [173] . El tránsito del *clicktivismo* (activismo de sofá a golpe de ratón) a un activismo real ha necesitado de un asentamiento completo de la doctrina neoliberal y de una profunda crisis económica en la que por primera vez desde el final de la segunda guerra mundial, tener empleo no es sinónimo de no vivir bajo el umbral de la pobreza[174].

[173] 16. VVAA. *Internet y Lucha política: Los movimientos sociales en la red*. Capital Intelectual, Buenos Aires, 2006

[174] 17. Kleim, N. *No logo. El poder de las marcas*. Booket. Madrid. 2011

2.3 Sistema mundial, producción y mercados

Como apuntábamos, las fusiones y la *sobredimensión* bursátil serán dos de las claves de la *nueva empresa*. Bajo el nuevo paradigma tecnológico se origina una forma diferente de organización sistémica, en la que el conocimiento y la información tendrán preeminencia, condicionando una forma de organización distinta, en red, de la mano de la revolución de la tecnología de la información.

Uno de los primeros indicadores del progreso económico, acudiendo a análisis económicos clásicos, será el de la productividad. Su aumento y su repercusión. Todos los análisis a los que se pueden acudir al respecto, asumen que a lo largo de siglo pasado, la productividad por trabajador ha ido en aumento, duplicándose en la producción no agrícola según el estudio para Norteamérica de Robert Solow. Este aumento en la productividad del trabajo ha sido una constante en las economías desarrolladas a lo largo de todo el siglo XX[175], y a pesar de los periodos críticos, ha sido uno de los principales factores de acumulación de la empresa productiva en occidente[176]. Sin embargo, este aumento no ha repercutido en los salarios ni la capacidad adquisitiva de los que trabajan sino que ha ido directamente a la cuenta de resultados empresariales. De hecho el empobrecimiento de la población y el empeoramiento de las condiciones de vida en general, y particularmente en España[177] han ido

---

[175] OIT, estadísticas sobre el empleo: http://www.ilo.org/global/What_we_do/Statistics/lang--es/index.htm

[176] Informes de la Comisión europea (EUROSTATS) sobre la productividad de la mano de obra: http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tsieb040

[177] INE: encuesta de condiciones de vida (actualizado a 2014) http://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176807&menu=ultiDatos&idp=1254735976608

aumentando sus cifras. Por otra parte, aunque el proceso fabril siga sacando provecho de la mano de obra masiva en la fabricación de ciertos productos, como sucede especialmente en China, la realidad de una sociedad mecanizada en la que el sector secundario reposa en procesos industriales se va imponiendo. Así el debate sobre la naturaleza del trabajo, su reparto y la reorientación de este en la nueva ha tenido un papel secundario, cuando debería haber sido la base de todo el proceso de cambios[178]. La respuesta oficial de organismos, gobiernos y gran empresa a este empobrecimiento paulatino, ha sido la elusión consciente del problema, la frivolización e incluso una respuesta agresiva. El espejismo de la clase media se enfrenta cada vez más a una devaluación a gran escala del trabajo asalariado[179]. El empobrecimiento de la masa laboral junto con la expansión de un crédito desligado de la economía real adquirirá la fuerza ideal para desembocar en una de las crisis más profundas de la edad contemporánea.

Por otra parte, el comercio internacional, al socaire de la globalización económica y las propias posibilidades de interconexión y comunicación entre empresas, que siguen representando la mayor parte del consumo internacional, muy por encima del de los consumidores particulares, ha crecido exponencialmente, en mayor medida incluso que la producción. Las directrices de la OMC, que finalmente representaban la mayor parte de los países desarrollados, implicarían que permanecer fuera de estas significaba permanecer al margen del comercio mundial. Esto implica la imposibilidad de modelos proteccionistas del tipo "sustitución de importaciones", que tantos países adoptaran en el pasado para proteger

---

[178] 4. Rifkin, J. *El fin del trabajo. Nuevas tecnologías contra puestos de trabajo: El nacimiento de una nueva era*. Paidós. Barcelona. 2004

[179] 5. Jones, O. *Chavs. La demonización de la clase obrera*. Capitán Swing. Madrid. 2012

sus mercados y potenciar la producción interna. Adoptar el modelo económico liberal se convertirá en condición casi irrenunciable de todas las economías nacionales, integradas en el sistema mundial que posibilita, en el proceso, el modelo expansionista de los que parten con ventaja. Como ya hemos visto, un solo sistema, con su óptica única y excluyente se impone como modelo económico y social.

Otro de los pilares de este periodo nuevo del sistema mundial es la forma en la que los mercados financieros se organizan. Por primera vez en la historia, los mercados financieros se han integrado por la vía de los hechos. Aunque existan diversas bolsas de valores los mercados funcionan a escala global de forma continua las 24 horas del día. Incluso se planteado por organismos como el FMI un proyecto de fusión de bolsas que integraría las de Nueva York, Frankfurt, Londres y la de Tokio, en una suerte de NASDAQ global y continuo. Los diversos mercados, juegan con ahorros e inversiones en tiempo real, con la capacidad de desplazar ingentes sumas de capital de forma casi instantánea. Las transacciones internacionales a gran escala han sido el otro gran factor en crecimiento y al igual que el comercio, presenta un gran desfase frente al del PIB de los países, siendo muy superior en todos los casos[180]. Esta sobredimensión lleva implícito la posibilidad de colapso, al estar cada vez más distante de un sustento productivo real. La propia naturaleza de los nuevos productos que se ofrecen, con la especial importancia que los valores sintéticos, conglomerados de acciones, bonos, opciones, moneda y materias primas de diversos países, dan sentido a esta volatilidad de los mercados. Una situación que ni siquiera la crisis declarada a partir de 2008 ha podido acotar. Tan solo los productos financieros cercanos a la burbuja inmobiliaria

[180] Dossier del FMI. *La globalización ¿amenaza u oportunidad?* : http://www.imf.org/external/np/exr/ib/2000/esl/041200s.htm

mundial han sido restringidos mientras el proceso especulativo sobre otros bienes, materias primas y productos de consumo como el cereal o el café incluidos.

La rotación de la propiedad de las acciones en EEUU ya a finales de los noventa era casi del 100%, es decir, que prácticamente la totalidad de los propietarios de títulos supuestamente los vendían en menos de un año. Todo este proceso, hace cada vez más apetecible la especulación sobe la inversión productiva, potenciando la inestabilidad de los mercados, sujetos a interpretaciones cada vez más "sutiles" como las de las agencias de calificación de riesgo, cuyos informes pueden llevar a movilizar capitales hasta precipitar procesos críticos a escala global. Son estos elementos de confianza, y no la vinculación productiva real, los que hacen que una empresa atraiga inversores, es decir, el juicio de valor del mercado financiero es el que realmente termina por condicionar el valor de las acciones de una empresa. El caso Amazon[181] es un ejemplo claro de esto. El valor de las acciones de esta página de venta por Internet era en 1999 más de 25.000 millones de dólares, cantidad que duplicaba el valor total de la bolsa rusa, hecho nada despreciable para una empresa que aún no había arrojado beneficios ni lo haría en los dos años siguientes. Ahora mismo, en virtud en gran medida de esa gran capitalización, la empresa es una de las grandes de Internet y no solo su venta directa desde su tienda, sino su librería o sus servidores cuyo tiempo puede alquilarse se encuentran encabezando sus respectivos sectores.

A pesar de esta enumeración de factores y su palpable inestabilidad, las recetas doctrinarias de los grandes agentes de la globalización, FMI y Banco Mundial, no hicieron más que potenciar este esquema en las zonas geográficas donde las sucesivas crisis acontecían y

[181] www.amazon.com

los gobiernos se veían abocados a pedir ayuda, que llegaba de la mano de la aplicación de las recomendaciones, imposiciones por la vía de los hechos, emanadas masivamente por economistas de la escuela neoclásica ortodoxa de la Universidad de Chicago, Harvard o el MIT. De todo este proceso, El FMI, a principios del presente siglo, gestionaba y asesoraba políticas de "ajuste" en más de ochenta países del mundo, lo que significaba, en definitiva, que se encontraban bajo la tutela y protectorado del organismo en cuestión; lo que en última instancia, como señala Castells, supone estar bajo las directrices del Departamento del Tesoro de Estados Unidos[182].

Europa no será una región marginada en el proceso sino que por contra, desde la propia unión europea se potenciará el mismo proceso de integración de mercados entre sus miembros, bajo un proceso de convergencia ideológica sin precedentes, que llevaría a la eurocámara a la aprobación de los tratados de Maastricht, que en 1999 supondría la efectiva unión económica y la progresiva apertura de mercados, no solo dentro de la unión, sino al exterior, con la promesa implícita de abandonar sectores enteros protegidos hasta entonces[183]. Este tratado, junto con la puesta en marcha de la moneda única y el Banco Central Europeo será una de las bases sobre las que profundice el proceso en el que la rentabilidad y la competitividad serán los motores de una economía globalizada[184]. Un proceso que culminará en una recesión y una quiebra del sistema del bienestar de la zona. Las denominadas "políticas de ajuste" acabarán con

---

[182] Castells, M. *La era de la información: economía, sociedad y cultura (Vol. 1): La sociedad red.* Alianza editorial. Madrid. 2008

[183] VVAA. *Geopolítica del caos*. Debate. Madrid. 1999.

[184] Palazuelos, E. *LA globalización financiera. La internacionalización del capital financiero a finales del siglo XX*. Síntesis. Madrid. 1998

los marcos regulatorios nacionales y buscarán un ensanchamiento de los márgenes de ganancia en todos los sectores[185].

En definitiva, todo este periodo de fines del siglo XX y todo lo que llevamos del presente, ha estado dirigido por el auge de lo que Ramonet denominara *Pensamiento único*, que ha supuesto la dominación ideológica del neoliberalismo, o neoconservadores en los Estados Unidos, que iniciaran su andadura en los ochenta con las políticas del tándem Thatcher-Reagan, con los patrones doctrinales de desregulación económica y social, privatización de todos los servicios estatales y apertura de todos los mercados a la "libre competencia"[186]. Esta receta ha llevado al triunfo de los mercados sobre los gobiernos, en una confluencia de intereses corporativos, de clase o grupo (rastrear a ciertos comisarios o altos cargos en sus posteriores funciones "privadas" sería ejercicio para toda una tesis), pero siempre en una sola dirección, que han cedido toda su soberanía, su capacidad efectiva de actuación en los mercados. La Nueva Economía, con sus formas y modelos empresariales, ha encontrado en camino expedito para medrar[187].

---

[185] 11. Arrizabalo de, X. *Crisis y ajuste en la economía mundial. Implicaciones y significado de las políticas del FMI y del BM*. Síntesis. Madrid. 1997

[186] 12. Ramonet, I. *Pensamiento único y nuevos amos del mundo*. Icaria. Barcelona. 2008.

[187] . Piketty, T. *La crisis del capital en el siglo XXI. Crónicas de los años en que el capitalismo se volvió loco*. Siglo veintiuno editores. Buenos Aires. 2014.

2.4 Modelos de empresa de la Nueva Economía

Como hemos visto en el caso Amazon y se ha apuntado en el capítulo 2.1 el modelo de empresa que inaugura esta nueva economía, sobre todo en sus ejemplos dedicados al comercio electrónico o que se mueven en los terrenos de lo virtual, dista mucho del esquema productivo que nos esperaríamos en un análisis clásico. Los cambios en el horizonte del mercado internacional, cada vez más integrado, bajo las pautas del liberalismo económico, el impulso de diversas instituciones internacionales y estatales en sentido único, la expansión de las nuevas tecnologías a cada vez más ámbitos, han llevado a un modelo productivo tan diferente del *fordismo* como del *toyotismo*, en el terreno de la creación de productos de consumo, como veremos, introduciendo elementos de flexibilidad en todas las escalas del proceso de producción.

El formato "Kan-ban" (justo a tiempo) [188] de adquisición de suministros, que prácticamente suprime el inventariado de almacenaje, condiciona a las empresas auxiliares a una mayor inestabilidad, dada su dependencia de una "central" solo vinculada por un contrato. La imposición de este modelo de empresa-red, supone una sincronización completa entre producción y comercialización. El neologismo "*glocalize*" define a la perfección este modelo de circulación y producción[189] . La parte más cruda

---

[188] Castells, M. *La era de la información: economía, sociedad y cultura* (Vol. 1*): La sociedad red*. Alianza editorial. Madrid. 2008

[189] 2. Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

de esta forma de organización es la del poder que las centrales que controlan el producto ejercen sobre unos productores que no tienen capacidad ninguna de influencia respecto a las empresas a las que sirven. En este contexto de fuerte explotación, en el que las condiciones laborales y la presión por producir con mayores márgenes (adelgazando la parte débil de la cadena como es la mano de obra), la divisoria de clases se establece a escala multinacional, correspondiendo el papel de "ajuste competitivo", a la coacción empresarial, a las ubicaciones con mano de obra masiva fuera, en principio alejadas de los lugares de gran consumo. De nuevo asistimos a uno de los puntos claves de la denominada Nueva Economía, como es que los grandes centros de decisión se ubican fuera del ámbito de la política y no pueden ser intervenidos desde los gobiernos locales. No solo se trata del poder de la gran empresa, sino también de los organismos (FMI, BM, BCE,) enfocados en una ideología de mercado en la que no hay lugar para exigencias en materias de derechos sociales[190] .

El control de los medios financieros y tecnológicos se convierten en la nueva base de la empresa red, como veremos, por encima incluso del proceso mismo de fabricación del producto final. La deslocalización no es un fenómeno nuevo, de hecho es una de las características básicas del modelo toyotista, pero en este caso, las nuevas formas de organización en red, distribuye y controla prácticamente en tiempo real toda la producción, reduciendo drásticamente los costes. Diversas tipologías de empresas están confluyendo hacia el modelo de empresa red, que emplea los vínculos horizontales, la colaboración o distribución productiva y la tecnificación y comunicación en tiempo real. Así encontraremos ejemplos

[190] 3. Ramonet, I*. Pensamiento único y nuevos amos del mundo*. Icaria. Barcelona. 2008.

no solo de las más tecnificadas sino como otros sectores como los de la construcción o el textil que han asumido estos principios productivos.

El cambio principal fue llevado a cabo desde la década de los noventa del pasado siglo en lo que se definió en su momento como "*producción escueta*"[191], basada fundamentalmente en el ahorro de mano de obra mediante la combinación precisa del control informatizado del trabajador, subcontratación de este y reducción de la producción. Ejemplos como los de la ATT en EEUU, o la propia Telefónica de España desde que iniciara su sendero privatizado, son casos muy esclarecedores. En este segundo ejemplo, que nos afecta localmente, solo tenemos que recordar el caso de los trabajadores de Sintel o las masivas prejubilaciones para sustituir trabajadores propios por subcontratas con iguales funciones. Ahora mismo, Telefónica, subcontrata prácticamente todos sus servicios, en un modelo que incluso resulta redundante tanto en tiendas comercializadoras como en empresas instaladoras, con la idea precisamente de mantener una variedad a la baja que repercute en lo que ha venido a definirse en el ámbito laboral como empresas "*cárnicas*"[192], dedicadas a prestar servicios en exclusiva a grandes empresas con empleo precario (jornadas supuestamente de menos de 8 horas con salarios al mínimo legal) de jóvenes recién titulados.

La contribución de la tecnología y el impacto de Internet en términos expresados en PIB, nos traerá unas cifras exponenciales, sobre todo teniendo en cuenta el momento crítico de la segunda década del siglo. Sin

---

[191] 4. Harnecker, M. *Haciendo posible lo imposible en el umbral del siglo XXI.* Siglo XXI (Ed), Madrid, 2000

[192] 5. VVAA. *Tus derechos en el trabajo*. Lulu Press. Morrisville. 2014

embargo estas cifras no significan que se produzca una transferencia en empleo[193]. El aumento de la productividad atribuible a la implantación del desarrollo tecnológico ha supuesto una transferencia en la acumulación de capital, mientras se continuaba la tendencia de adelgazamiento laboral[194]. Este panorama abunda en la interpretación acerca de la forma en la que se está gestionando esta nueva economía, cuya eficiencia es puesta en entredicho cuando se humanizan las cifras y los resultados[195]. En España, coincidiendo con el periodo de mayor ahondamiento en las cifras del paro y el empeoramiento generalizado de las condiciones de vida de sus habitantes[196], se alcanzarán cifras de impacto directo de Internet del 4% del PIB en 2009 y un aumento del 14% anual, lo que pone de manifiesto el desfase entre una economía en movimiento y una realidad social en proceso de pauperización paulatina y decrecimiento de sus capas medias[197].

---

[193] Rifkin, J. *El fin del trabajo. Nuevas tecnologías contra puestos de trabajo: El nacimiento de una nueva era.* Paidós. Barcelona. 2004

[194] OIT, estadísticas sobre el empleo: http://www.ilo.org/global/What_we_do/Statistics/lang--es/index.htm

[195] Ugarte de, D. *Los futuros que vienen*. Colección Biblioteca de las Indias. Madrid. 2010

[196] INE: Encuesta de condiciones de vida en España (actualizado a 2014) http://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176807&menu=ultiDatos&idp=1254735976608

[197] Informe España Conecta. *La transformación dela economía española a través de Internet*: http://www.espanaconecta.es/informe/ (patrocinado por Google y The Boston Consulting Group- BCG)

De la deslocalización a la "compañía hueca"

La manifestación extrema de esta nueva forma de entender la producción será la denominada "compañía hueca", como empresa especializada en la intermediación entre financiación, la producción y las ventas al mercado. Esta será otra de las características de muchas firmas de prestigio, sobre todo en marcas de dispositivos electrónicos, que utilizan a las denominadas marcas blancas como fábricas propias para vender el mismo producto a sobre costo al colocarles el identificador propio, como hará HP con marcas como ASUS o COMPAQ, o IBM con Lenovo, en principio (la historia de estas dos últimas merecería un análisis aparte). El modelo cundirá entre ciertos centros de prestigio que otorgarán su marca en occidente de un producto generalmente producido en China. Hasta la primera década del siglo XXI, donde la concentración empresarial "depuró" buena parte de la variedad de marcas, resultaba común encontrar el mismo producto comercializado por diversas marcas con precios también muy diferentes.

La estructura de red también ha traído una nueva forma de integración de mercados, en los que no es la gran transnacional del esquema clásico al que todos acudimos, que se ubica en una región de destino y comienza a producir, la que prima. La estructura en red, ofrece un vínculo concreto de pequeñas y medianas empresas de la zona, con sus propios procesos internos, respecto a una matriz con la que suele mantener una exclusiva de producción. En este aspecto la red de empresas es una forma sutil de penetración en mercados locales y viene a suponer el reverso del modelo antes expuesto de producción fabril de la gran empresa, dado que se orienta a penetrar estos mercados locales con el producto de esta gran empresa, no solo ya desde el modelo franquiciado sino permitiendo la

coexistencia de una comercialización propia. En realidad es una forma sutil de llegar a mercados de más difícil acceso mediante la alianza local y la comunicación permanente y asimismo sacar provecho de ayudas públicas y exenciones en diversos aspectos [198] . En el terreno tecnológico, se identifica en muchos aspectos con el denominado "Parther Local", en forma de aliado en la extensión de la gran empresa en ubicaciones en las que esta no ha proyectado su organización por diversos motivos.

Por otra parte, son estas redes de empresas las encargadas de innovar y adaptarse, sin excluir financiación pública o investigación por parte de universidades de los diversos estados, mediante proyectos de I+D, a diferentes escalas, que finalmente revierten en la organización en su conjunto. La unidad operativa actual es el proyecto empresarial no las empresas concretas o las agrupaciones de estas, organizada de forma horizontal en forma de red dinámica descentralizada, adaptada al cambio dado que la supresión de partes concretas de esta se pueden realizar sin costo ni dilación alguna.

Entre los ejemplos que podemos emplear para identificar empresas-red, el caso de Cisco Systems[199] es uno de los más destacados. Empresa ubicada en San José, California, Cisco es la proveedora principal de todos los equipos conmutadores, concentradores y direccionadores (Switches, Hubs y Routers) necesarios para la arquitectura de redes en todas las escalas. Sus equipos forman parte de la principal infraestructura

---

[198] Pérez, C. *Las nuevas tecnologías: Una visión de conjunto. En La tercera revolución industrial (Impactos internacionales del nuevo viraje tecnológico).* Rial, Buenos Aires. 1986.

[199] La compañía CISCO es una de las piezas claves en el despliegue de la infraestructura de red mundial: http://www.cisco.com

de red, con una cuota del 80%, hasta el punto que obtener el certificado de especialista en redes CISCO, *CCNA (Cisco Certified Network Associate)* es una de las bases de cualquier técnico de sistemas informáticos, por encima incluso de otras titulaciones concretas[200]. La empresa fue creada en 1985 por dos profesores de la universidad de Standford, con la aportación inicial del 2 millones de dólares por parte de un financiero de capital riesgo. En 1986, lanzaría su primer producto, consiguiendo unos ingresos anuales de 69 millones de dólares, comenzando a cotizar en bolsa en 1990. Para el año 1999 sus beneficios ascendían a 12.200 millones de dólares. Entre el año 1995 y 1999 su valor bursátil había aumentado un 2.356%, alcanzando un valor de 222.000 millones de dólares y convirtiéndose ya en la quinta mayor del mundo, unas cuatro veces el valor del gigante industrial General Motors en ese momento[201]. Las claves de este éxito[202], están tanto en la oportunidad del momento, cuando toda la infraestructura ya había sido diseñada para funcionar en unos estándares y se encontraba en pleno proceso de expansión e instalación, como en la "audacia" comercial de la compañía, que comenzaría desde sus inicios una campaña de adquisiciones de empresas del sector y de inversión en I+D, pero sobre todo la subcontratación y el trabajo en red. Para ello, la imagen de empresa innovadora, competitiva y rentable, con un nuevo modelo empresarial, resultó ser prácticamente un valor más en cuanto a la atracción de inversores. La empresa, aplicaría el mismo modelo reticular de producción que aplicaba a sus clientes, con unos parámetros de gestión on-line que automatizaban buena parte del proceso de relación entre clientes,

---

[200] Certificado en redes y equipamiento cisco: http://www.cisco.com/web/learning/le3/ccie/index.html más información en castellano http://certificacionescisco.blogspot.com/

[201] . Información financiera actualizada en *Google finaces*: http://www.google.com/finance?q=NASDAQ:DELL

[202] Castells, M. *La era de la información: economía, sociedad y cultura* (Vol. 1*): La sociedad red*. Alianza editorial. Madrid. 2008

proveedores, socios y empelados. De hecho, en 1999, Cisco solo era propietaria directa de dos plantas de producción, de las treinta que fabricaban equipos para la compañía, empleando solo a 23.500 trabajadores, casi la mitad en su matriz de San José, entre ingenieros, investigadores y gestores. La práctica totalidad del negocio se realiza en la red, de forma *on-line*, con un sistema de pedidos diseñado para que el cliente disponga de múltiples opciones y donde solamente las grandes operaciones se realizan bajo seguimiento personal. Si se desea ese tipo de trato para otro tipo de compras supondrá un costo adicional por parte del cliente. Una vez realizado el pedido, el propio sistema encamina este a la red de proveedores, que envían directamente el producto al cliente. En 1999, ya gestionaba la empresa el 83% de sus pedidos a través de la red, y al mitad de estos se transmitían a través de su red de subcontratistas, que las entregaban directamente. Analizando estos datos, nos encontramos con el más claro ejemplo de nueva empresa en red, una compañía que, dedicada a la manufactura de productos electrónicos, apenas fabrica hoy en día, sino que gestiona la información de una gran red comercial, tejida entorno a su *Website* (página central), desde donde gestiona prácticamente todo el proceso de su negocio. Otro de los grandes pilares del éxito tan contundente de Cisco, como ya apuntábamos, ha sido la generación de confianza entre sus inversores, auspiciada por sus cuentas de resultados y una política de alianzas con las compañías destacadas del sector, en la mayor parte de sus vertientes; desde proveedoras de servicios como US West o Alcatel, servidores con tecnología Intel, Hewlet Packard (HP) y software de Microsoft y otras integradoras de sistemas. Como hemos señalado, una precisa gestión reticular y una acertada política de alianzas, han hecho de esta compañía, que en principio no contaba ni con los recursos, conocimientos ni el tamaño para ser cabeza del sector, en uno de los grandes negocios de nuestro tiempo y en una presencia casi ubicua en el sector concreto de las infraestructuras de red.

El ejemplo de Cisco, es uno de los más destacados por ser paradigma del modelo de nueva empresa red de nuestro tiempo, aunque otras compañías, ya habían ensayado el formato on-line, como Dell Computers(15), que en los noventa ya comenzó a destacar en el mercado de los ordenadores personales, con una página que permite personalizar el pedido de la máquina que pretendemos comprar en muchos elementos, partiendo de una base, para finalizar el pedido en un proceso libre de intervención por parte de la compañía. Al igual que la empresa anterior, Dell tendría un vertiginoso ascenso de su valor bursátil del 9.400% entre 1995 y 1999[203].

Otras empresas del sector con mucha más trayectoria, como es el caso de Hewlet Packard [204], se adaptarían pronto a este modelo. Paralelamente a la venta diversa de equipos, desde sectores empresariales hasta el ámbito doméstico, HP organizaría un nuevo negocio mediante el que alquilaba potencial de sus servidores a través de la red, ofreciendo herramientas de venta on-line a sus clientes a cambio de un porcentaje de los beneficios. En un proceso paralelo, continuó aumentando la subcontratación de buena parte de la producción, sobre todo a compañías asiáticas, como Asus, sin dejar de lado la posibilidad de absorber a la competencia, como hiciera con COMPAQ, cuyas fábricas pasarían a ser fabricantes de ordenadores y otros productos de electrónica de consumo, aprovechando la experiencia de esta.

Sin querer extendernos en las prácticas empresariales de estas nuevas compañías, en esencia bastante similares, podemos señalar como no solo el sector tecnológico se ha adaptado a este modelo. Cuando aseguramos que las prácticas de la nueva economía se suponen un patrón

---

[203] El Índice Nasdaq, pasaría de ser uun indicador bursátil de tecnolo´gias punteras a covertirse en el referente principal del conjunto económico mundial: http://www.nasdaq.com/

[204] HP es otra de las grandes del sector: http://www8.hp.com/es/es/home.html

diferenciado en el sistema mundial es porque su modelo se ha extendido a otros sectores. Pronto otras empresas de sectores diversos hace uso de sistema reticular, desde el de la maquinaria agrícola, John Deree, el comercio de la alimentación, o la fabricación automovilística, caso de Renault, pasando incluso por el pantanoso terreno de la educación, como más adelante comentaremos. Dado que finalmente son las cuentas de resultados y la valoración bursátil (factores cada vez más unidos y equiparados) los objetivos de las empresas, la extensión de este patrón continuará. La mayor empresa de construcción de edificios en San Francisco, *WebCor*, ha organizado la mayor parte de su labor de desarrollo a través de su página Web y los elementos subsecuentes de esta, con todo el software orientado al uso compartido disponible en la actualidad, (CAD, GIS etc.). Mediante la implementación de esa tecnología ha sido capaz de reducir a la mitad el tiempo de producción de un edificio, con un tercio del personal de gestión, limitando los costes en un 50%.

Para terminar con un ejemplo más cercano, señalaremos cómo ZARA con 2001 almacenes en el mundo, en treinta y cinco países diferentes, se ha convertido en otro de los ejemplos de empresa gestionada con los patrones de la empresa red[205]. Cada compra que se realiza, es registrada en una gran base de datos general que comunica todos sus centros mediante informes semanales desde cada uno de estos a la central coruñesa, donde un equipo de 200 diseñadores procesa todos los patrones para fabricar ropa y los envían directamente por la red a todos los centros de producción. Con este sistema de comunicación electrónica y procesado

[205] . Castells, M. *Lliçó inaugural del programa de doctoral sobre la societat de la informació i el coneixement*:http://www.uoc.edu/web/cat/articles/castells/print.html

de datos, ZARA ha conseguido reducir a dos semanas el tiempo necesario para rediseñar un producto y ubicarlos en sus centros de venta distribuidos por todo el mundo, desbancando a el modelo más parecido de red no informatizada del periodo anterior, como fuera Benetton, que concentró horizontalmente una serie de empresas del sector.

En definitiva, al igual que el fordismo y en parte luego, el toyotismo, modificaron el esquema de producción industrial, la adaptación tecnológica de las compañías y el modelo aparejado a estas, al abrigo de la mundialización y la doctrina neoliberal, está propiciando un acelerado proceso de cambio de modelo no solo en las que desde el principio se dedicaron a la red o las denominadas nuevas tecnologías sino en todos los terrenos de la producción, trasladando cambios en los terrenos sociales y laborales. Unido a esto, el mundo financiero también vive un momento de expansión que lo ha llevado a adquirir un papel preponderante en muchos aspectos, con la capacidad de trastocar la "economía real" en mano de tendencias especulativas.

2.5 Una legalidad "removible" frente al monopolio

La paulatina concentración empresarial y las prácticas monopolistas han sido uno de los elementos iniciales de diversas compañías tecnológicas, con casos como los de ATT, IBM o Microsoft, que nos han demostrado la ductilidad de la legislación cuando se trata de compañías de tanto peso y nos indican el camino descendente, desde la crudeza del primero hasta la práctica "nulidad" del tercero. La ambivalencia del proceso en el que mientras que los grandes sectores estatales, sobre todo en Europa, son privatizados, las mismas leyes sobre la concentración empresarial entran en conflicto con estos gigantes, obligando a salidas en ocasiones truculentas.

Por otro lado la posición de dominio de ciertas compañías del sector a lo largo de la historia de Internet ha conseguido que sus procesos judiciales hayan sido resueltos de formas muy diferenciadas. La posición dominante de EEUU y la defensa de sus grandes compañías, empeñadas en campañas lobistas mediante las que apuntalar dicha defensa. Algunos escenarios demostraran claramente esta afirmación, como los casos en los que se negociara el gobierno de Internet, en las negociaciones de la UIT, ejemplos como los de la fiscalidad de empresas como Apple o Amazon, que por ejemplo en Europa buscan tributar en Irlanda para burlar los impuestos de cada país o como veremos, las situaciones más recientes de Google o Facebook, respecto a las noticias o el reconocimiento facial de sus usuarios.

IBM cerrando el paso

El primer gran caso contra prácticas monopolísticas sería el de IBM (International Business Machines Corp)[206], cuando en 1969 Lyndon B Johnson, iniciara un proceso contra una compañía acusada de prácticas restrictivas de la competencia, en un momento en el que controlaba las tres cuartas partes del mercado informático del país. El caso judicial duraría hasta 1983 y condicionaría parte de la política de la empresa desde aquel momento, acusada de constreñir, algo similar al posterior caso de Microsoft, el sistema operativo a la máquina (ligando software con hardware) de modo que limitaba la capacidad de la competencia, que prácticamente quedaba excluida.

El ingente proceso de instrucción contra la compañía quedó finalmente abandonado, después de que una nueva administración republicana llegara al poder y defendiera la causa abierta por la entonces CEE, dos años más tarde, después de un largo y azaroso itinerario, aunque, como hemos señalado, sería importante en tanto que restringiría ciertas tendencias empresariales que después tendría consecuencias inesperadas. Efectivamente, el focalizar buena parte de la demanda en caso específico del software de la máquina, posibilitaría que el desarrollo del PC fuera un elemento susceptible de ser clonado por el mercado asiático, de donde procedían, por otra parte, la mayoría de los componentes, dado que IBM no había desarrollado estos sino que los había ensamblado por medio de diversas fuentes baratas con el objeto de que el IBM-PC no fuera competencia efectiva a su mercado de servidores. Como el sistema operativo tampoco era un desarrollo propio sino un encargo a

[206] Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

Microsoft, otra historia azarosa, la pronta aparición de PC compatibles, a los que esta última vendería licencias de su sistema operativo, popularizaría este modelo de ordenador doméstico a precio relativamente asequible.

Un mercado de telecomunicaciones sin competencia

En 1972, Gerad Ford, sucesor de Nixon en la presidencia de EEUU, iniciaría otra campaña antitrust contra el gigante de las telecomunicaciones AT&T (American Telephone and Telegraph)[207], casi una enseña del modelo norteamericano y un monopolio de las telecomunicaciones a la largo de los tres primeros cuartos del siglo XX, con el beneplácito del gobierno, acordado en el llamado Compromiso Kingsbury[208]. La administración Charter (1976-1980) sustituiría la Office of Telecomunications Policy por otra agencia a cargo de la autoridad de la Secretaría de Comercio, la NTIA (National Telecommunications Policy Information Administration), como forma de reconducir toda la política de telecomunicaciones en su conjunto, definida en la *Communication Act,* con el objetivo claro de poner fin al monopolio del AT&T para abrir el mercado de la competencia en el sector y acabar con la idea de monopolio afín y regulado mediante acuerdos, aspecto defendido sobre todo por el Departamento de Defensa y sectores del partido republicano.

En enero de 1982, Bajo la presidencia de Reagan, culminaría el proceso con la decisión de dividir la compañía en ocho diferentes

---

[207] AT&T sigue siendo una compañia líder del sector: http://espanol.att.com/

[208] Sobre el monopolio de AT&T http://morfeo.upc.es/crom/mod/wiki/view.php?id=4&page=view/Monopolio+de+AT&editor=dfwiki&gid=0&uid=0

empresas, siete de las cuales continuarían como operadores regionales Bell, conocidas como "Baby Bells" (Pacific Bell, SouthwesternBell, Nynex y Bell Atlantic , BellSouth y Ameritech), nombre tomado de la división de desarrollo de la matriz, Laboratorios Telefónicos Bell (Bell Labs), con el que se conocería a estas compañías emancipadas que en principio heredaron el monopolio en las diversas regiones asignadas[209]. En 1996 una nueva Telecommunications Act, a cargo de nuevo de la FCC (Federal Commnunications Commision)[210], sentaría los cimentos de las leyes de la competencia en el sector, en el que no han parado de darse demandas cruzadas. De cualquier modo, AT&T, tomaría buena nota del proceso y en el mismo año tomaría la decisión voluntaria de separar tres de sus divisiones concretas en empresas especializadas: Lucent Technologies, fabricante de equipos, sobre todo en el terreno de las telecomunicaciones (heredero directo de los laboratorios Bell) NCR, fabricante de equipos absorbido años antes y nuevamente liberado en esta operación, y otra AT&T más pequeña y enfocada a las telecomunicaciones exclusivamente, que pronto absorbería al segundo operador de televisión por cable y otras compañías de telefonía.

Respecto a las otras siete divisiones regionales, pronto entrarían en un proceso de fusiones y adquisiciones, lo que supuso que, el efecto real de este proceso no empeorarían en nada a cada una de las divisiones de la empresa sino que todas, en su conjunto saldrían beneficiadas al partir, de cualquier modo, de posiciones ventajosas en el mercado.

---

[209] La división y todo el proceso de disgregación del gran monopilio estadounidense de telecomunicaciones queda muy bien documentado en la obra de Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

[210] FCC: http://www.fcc.gov/telecom.html

Curiosamente, en un momento en el que las telecomunicaciones han pasado a primer plano, apenas tres operadoras se disputan el grueso del mercado de telefonía móvil en nuestros días. En el ámbito doméstico, en un momento de precios ajustados, sí que se ha vivido una conversión tanto de los operadores de cable como de otras compañías en un mercado convergente en el que desde hace mucho los servicios de voz son una parte anecdótica, teniendo en cuenta que la mayor parte del flujo se hace mediante protocolos de datos. Como apunte anecdótico*, Google Fiber*, el servicio de fibra óptica de Google que ofrece un gran caudal de datos a precios muy contenidos se ha convertido en el nuevo enemigo de todo el conjunto de operadoras preexistentes, apuntando al dato, como fuente real del negocio.

El gigante Microsoft

El tercero de los ejemplos, el de Microsoft, es algo diferente en cuanto que en él se unen diferentes procesos, que llegan casi de forma recurrente a lo largo de los últimos veinte años, junto con otras políticas de empresa discutible pero circunscrita al ámbito "legal". Como ya señalamos, la discutible política de Microsoft, desde sus orígenes, iniciada por Bill Gates y Paul Hallen, respecto a la imposición de medios concretos y la primacía del negocio, anulando competidores sobre la innovación, han convertido a esta compañía en una de las más impopulares de los medios informáticos y el punto de mira judicial de diversas instituciones[211].

[211] El famoso abogado y activista Ralph Nader, recopilaría todo el proceso llevado adelante durante 1997 contra las prácticas del gigante del software Microsoft. Nader, R. *Appraising Microsoft*: http://www.appraising-microsoft.org/1st.html .

Sin querer extendernos en un tema que por sí solo ha llenado titulares de prensa apuntaremos los casos más reseñables abiertos contra Microsoft y sus acciones más rechazadas. Comenzaremos con la propia génesis de su sistema operativo inicial, que dará inicio a su negocio. Con el encargo de IBM de crear un sistema operativo para integrar en sus máquinas PC-IBM, después de fracasar en sus negociaciones con la compañía Digital Research, Microsoft compra al programador Tim Paterson[212] su desarrollo QDOS (Quick and Dirty Operating System-Sistema Operativo Rápido y Sucio) y lo contrata para su adaptación a la nueva máquina, mientras adquiere de Seattle Computer Products la licencia, sin exclusividad, de un clon de CP/M llamado 86-DOS[213]. IBM, apremiada por las fechas de lanzamiento ya prefijadas seguirá el proceso de desarrollo casi a diario. Finalmente Microsoft licenció QDOS a IBM, y bajo el nombre de PC-DOS y con una licencia no exclusiva y un mes antes de lanzamiento comercial de las primeras PC-IBM, adquirirá todos los derechos de 86-DOS de *Seattle Computer Products* por 50.000 dólares, para garantizarse el siguiente movimiento. Efectivamente, la posibilidad de clonado de estas máquinas abriría el mercado a la venta de un sistema ya adaptado a estos, redenominado para la ocasión como MS-DOS. Desde Digital Research, se discutiría este sistema operativo, al observar la similitud tan absoluta con la interfaz de programación de CP/M, tratando de llevar adelante una demanda contra IBM, que finalmente no prosperara.

---

[212] Patterson sigue dedicado al desarrollo de productos informaticos: http://www.patersontech.com

[213] El propio Patterson nos narra desde su perspectiva cómo sería el proceso de adquisición y uso de QDOS: http://www.patersontech.com/Dos/Byte/History.html

Los dos siguientes capítulos, ya señalados, en el caso de Microsoft vendrán de modo casi simultaneo de la mano, por un lado de los sistemas operativos, con un remedo del desarrollo de interfaz gráfica que Xerox PARC (*Palo Alto Research Center)* realizara para los nuevos ordenadores de Apple, y por el otro de los navegadores, con el caso de la redenominación de la ideal de creador de Netscape, Mosaic, para llamarlo Internet Explorer y distribuirlo exclusivamente en sus nuevos sistemas operativos Windows 95. A partir de este momento, los procesos judiciales se irán sucediendo en una carrera contra el tiempo, dado que, mientras las demandas se demoran, las prácticas de Microsoft terminan por imponer por la vía de los hechos sus pretensiones[214].

En 1991, la Comisión Federal del Comercio inicia un expediente a Microsoft sobre prácticas monopolísticas en el mercado de sistemas operativos para PC. En 1993, mientras la fiscalía nacional cierra el expediente, el Departamento de Justicia y la Comisión Europea, inician sus propios procesos, a lo que Microsoft responderá eliminando algunas de las restricciones impuestas a fabricantes de software. El caso seguirá un azaroso cauce en el que se demostrará cuanto está en juego y la capacidad de penetración del lobby sobre el que actúa Microsoft. En 1995 el caso será reabierto por la corte de apelaciones, después de haberse tratado de nuevo de archivar. En 1997, una nueva demanda se entabla contra la compañía, bajo la acusación de violar el acuerdo de 1994, al obligar a los fabricantes de equipos que preinstalan el sistema operativo Windows 95 en sus ordenadores, a incorporar con este el navegador *Internet Explorer*.

---

[214] Paterson, T. *From the Mailbox: The Origins of DOS:* http://www.ece.umd.edu/courses/enee759m.S2000/papers/paterson1994-kildall.pdf

La Comisión Europea abre asimismo otro expediente relativo al mismo caso, al tiempo que el fabricante COMPAQ (antes de su absorción por HP), denuncia la pretensión de Microsoft de anular su licencia de Windows 95 al no instalar con este su navegador. La compañía incluso acusa al Departamento de Justicia de impedir el desarrollo de su sistema operativo, a lo que este responde con la acusación de que lo que está haciendo la compañía es integrar su navegador dentro de sus sistema operativo, como forma de aprovechar su posición dominante en estos para llevar a sus usuarios a que desplacen a Netscape. Mientras tiene previsto el lanzamiento de Windows 98 con el navegador integrado en el propio sistema operativo, indistinguible del explorador interno, abre la posibilidad de que los fabricantes anulen la instalación del navegador en su sistema anterior (Windows 95), en una estrategia dilatoria para que no se prohibiera el lanzamiento de este, como pretendían algunos jueces. A finales de 1998, Netscape, desplazado del mercado de los navegadores, es adquirido por el proveedor de servicios de Internet AOL (América On-line), por unos 10.000 millones de dólares. Para Noviembre de 1999, el Juez Thomas Penfield Jackson, a cargo del nuevo sumario, publica las primeras conclusiones del sumario, en el que se acusa a Microsoft de prácticas de monopolio e imposición a otras compañías, acudiendo a tácticas de presión para anular competidores, distorsionando conscientemente cualquier posibilidad de competencia real, además de entrar en otras áreas de negocio con las estas mismas prácticas. Inmediatamente, esta responde tratando de abrir negociaciones para llegar a un acuerdo. El solo hecho de este anuncio hace subir la cotización de la compañía un 6%. De cualquier modo, el 31 de mayo de 2000, dictaría una sentencia en la que obligaba a la compañía a dividirse en dos divisiones diferentes, a lo que esta apelaría inmediatamente[215]. Una vez en la Corte de Apelaciones, el caso volvería a

[215] Un seguimiento pormenorizado del caso Microsoft podemos encotrarlo en: http://www.noticiasdot.com/publicaciones/2002/1102/021102/noticias021102/noticias021102-2.htm

convertirse en una ceremonia de la confusión, revocando la división pero ratificando las conclusiones, nombrándose por dos veces juez instructor, el último de los cuales trata de devolver el caso a juzgados de distrito. El propio gobierno estadounidense, a través del Departamento de Justicia, señala que no buscará la división de la compañía. Mientras tanto, la unión europea continúa su proceso y abre una nueva causa respecto al mercado de los servidores y en concreto los orientados al comercio electrónico, mientras amenaza con una multa de 2750 millones de dólares si no elimina los componentes adicionales de su sistema operativo que impiden la competencia.

Mientras tanto, en octubre de 2001, con la impronta ya de la nueva administración Bush, el Departamento de Justicia y Microsoft llegan a un acuerdo, que suscriben otros estados, quedando nueve de los acusadores sin suscribir el acuerdo, aunque finalmente no prosperara el caso[216] [217] . Otros tres casos, contra Caldera Systems, por verse expulsada del sistema de servidores, Sun Mycrosistems, por acusar a Microsoft de modificar JAVA (programa multiplataforma para ejecutar aplicaciones sin importa el sistema operativo) y Bristol, que al no contar con el código fuente de su sistema operativo no pudo adaptar sus productos, quedando expulsado del mercado dominante, se resolverían con millonarias sanciones que la compañía, con su habitual política de hechos consumados, pagaría cuando ya se había beneficiado del asunto. Los casos que quedarían serían los de la Comisión Europea, que mediante sanciones económicas, o con la división en diversas versiones del sistema XP, como fuera en el caso de la inclusión del reproductor de medios Windows Media Player, abierto en

---

[216] http://www.usdoj.gov/atr/cases/ms_index.htm

[217] http://www.usdoj.gov/atr/cases/f3800/msjudgex.htm

2004, serían resueltos teniendo como único beneficiario real, a pesar de las sanciones, a esta compañía.

Con la nueva década, la propia compañía será la que mediante sucesivos errores y una falta de perspectiva respecto a los dispositivos móviles y el auge de una red en la que el dispositivo y por tanto la venta de un software fijado en una máquina cada vez importa menos irá perdiendo liderazgo. Nuevos sistemas operativos en el terreno móvil, como iOs, de Apple y Android, libre aunque de la mano de Google, junto con los navegadores Mozilla Firefox, de la fundación Mozilla, y Chrome, de nuevo de Google, desbancarán los desarrollos de la gran empresa de Redmon. Así, en un periodo de tiempo no muy dilatado el gran monopolio de Microsoft en sistemas operativos, navegadores e incluso en sistemas de gestión documental, quedará puesto en entredicho.

Como hemos apuntado al inicio, los casos contra diferentes posiciones de fuerza, monopolio o abuso, serán una constante y los "nuevos grandes" de Internet, Amazon, Apple, Facebook o Google, entre los más destacados, acumularan cada cual una buena cantidad de litigios en los que demostrarán que no se trata de actores al uso sino que tienen capacidad para entablar negociaciones directas con naciones o estamentos supraestatales. Si bien es cierto que la última gran causa contra un monopolio será la de Microsoft y que tanto por parte de las administraciones como mediante una estrategia diferente por parte de estas grandes empresas, se ha cambiado la forma de encarar estos procesos, la realidad es que el proceso de concentración de recursos y la destrucción de competencia sigue un curso ascendente. Entre la estrategia más empleada por estas empresas, se ha creado una especie de mercado de nuevas plataformas y productos que surgen mediante inversiones de capital riesgo y se enfocan hacia la adquisición por estas grandes. Por otro lado, no hay lugar para competir en ciertos nichos,

colmadas hasta tal extremo que no hay posibilidad real de hacerse un lugar propio. Así, parte de los departamentos de innovación se han convertido en un departamento de adquisiciones, mediante el cual agregar innovación mediante la adquisición de productos que funcionan. Por nombrar uno de los ejemplo paradigmáticos, señalaremos cómo Google adquiriría la competencia real de Google Vídeo (el portal de vídeos en internet), YouTube, para integrarla en sus servicios y unificar ambos[218].

A pesar de tener consciencia del coste real para una economía de este nuevo sistema de monopolios[219], máxime si quiere arrogarse la defensa de un mercado libre, a lo largo de la última década las instituciones internacionales han avanzado poco en poner límite a estos. De hecho, muchos gobiernos ceden ante la presión de estas grandes compañías que ejercen cada vez un mayor poder lobista sobre los responsables públicos. En el parlamento europeo no era tan común como en los EEUU la presencia de grupos lobistas que trataban de ejercer su influencia respecto a los representantes públicos que atesoran la expresión de poder popular de las democracias que los han elegido. Merecería todo un debate delimitar hasta qué punto esta influencia resulta distinguible de la corrupción.

---

[218] Suárez Sánchez Ocaña, A. *Desnudando a Google*. Deusto. Madrid. 2012

[219] Informe de la Asociación de telecomunicaciones británica sobre la seguridad y el coste del monopolio en las grandes redes. *Cyber*In*security: The Cost of Monopoly:* http://cryptome.org/cyberinsecurity.htm el peligro para la seguridad del monopolio de Microsoft, algo que con el tiempo quedaría demostrado en casos como el de Lituania (como veremos mas adelante)

2.6 La red como mercado de burbujas

Una de las características iniciales de las empresas orientadas a la red ha sido la de su capitalización. Como compañías surgidas en un contexto histórico concreto, la influencia de las formas de financiación, del capital riesgo y la inversión sobredimensionada será una de las características más referidas desde sus primeras fases. Desde la crisis de las *puntocom*, y la primera crisis mejicana y japonesa, hasta la gran crisis financiera iniciada a partir de 2007, las empresas tecnológicas y vinculadas con Internet han estado en el epicentro de buena parte de estos estallidos especulativos.

El periodo 1997-2001 fue uno de los primeros en los que la capitalización bursátil enfocaría sus apuestas hacia un sector tecnológico en fuerte desarrollo[220]. El índice NASDAQ de Nueva York, que es la referencia tecnológica y el indicador del pulso económico de la denominada Nueva Economía recogería unos crecimientos espectaculares. Los capitales riesgos concurrían en una carrera por "ocupar espacios", llegar primero en una carrera por tener una posición predominante en un futuro crecimiento que se preveía, aunque todavía no se cimentaba en datos y resultados reales. La retroalimentación que los mismos medios otorgaban a las entonces empresas pioneras, como *Amazon* (que tardaría un quinquenio en conseguir beneficios) o el portal español *Terra*, desligado de telefónica para cotizar en bolsa de forma independiente[221]. Era el tiempo de los grandes portales, en los que la red era dirigida y más que buscar contenidos, estos los suministraban de forma

[220] 1. Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

[221] 5. Kleim, N. *No logo. El poder de las marcas*. Booket. Madrid. 2011

sesgada. En ese momento, Google era una anécdota frente al dominio de Yahoo! Lycos o AltaVista, todos ellos muy vinculados al sistema de "portal de internet" en donde se ofrecían unos contenidos variados con el que copar los escasos anchos de banda del momento. El modelo B2C (Bussines to Customer), que planteaba Internet como el centro de venta sin intermediarios todavía tenía un largo camino por recorrer y una madurez por alcanzar que no se había producido aún, aunque tanto las "apuestas" como las predicciones más sensatas apuntaban hacia ese futuro de abaratamiento de productos de consumo por la vía de la venta directa, el momento estaba por llegar y la gran movilización de capitales apuntando hacia un valor futuro por determinar terminaría por enfrentarse a la realidad de los resultados y el abismo de la rentabilidad inmediata[222].

Como hemos comentado en capítulos previos, el paradigma de esta burbuja sería la compra de Time Warner, el mayor conglomerado de medios y producción audiovisual de EEUU por parte de los proveedores de servicios de Internet AOL (América Online) por 160.000 millones de Dólares. Es decir, que una empresa sobrevalorada juega con la inversión recibida para apoderarse de grandes medios productivos.

Entre el momento máximo de esta primera burbuja, alcanzado el 10 de marzo del año 2000, cuando el índice NASDAQ alcanzaba un récord de 5.048,62 puntos, hasta su desplome de 1.114,11 puntos a principios de octubre de 2002 se produce un desplome de la imagen banalizada que unos medios "analógicos" vendían de este Internet "que venía", comercial y privado. El modelo heredaba en buena parte la óptica del gran dominador del negocio informático del momento, Microsoft, que vendía sus productos

[222] Recopilación de la revista *Wired* sobre la época*: A los 10 años de la Burbuja .com*: Archivo PDF disponible en http://www.wired.com/2010/02/10yearsafter/.

vinculados a una "maquina" con la que el usuario interactuaba y le daba acceso a una red muy limitada en ese momento.

Salvo Amazon, cuyo modelo estaba por desarrollar y que si sería un caso de éxito hasta convertirse en una de las grandes compañías de la actualidad, empresas como Cisco, Microsoft e Intel no recuperarían los valores que tenían el año 2000 hasta bien pasado una década. Se estima que prácticamente el 50% de las compañías del puntocom, no sobrevivieron a la crisis.

Uno de los errores del periodo fue pensar en Internet como en una frontera en la que los principios clásicos de la empresa se aplicarán de forma automática. La proliferación de banners publicitarios, pop ups y la profusión de clips insertados, producidos con Macromedia Flash son testimonio de un periodo tan exuberante como desacertado[223].

Para comprender la formación de la web posterior a la burbuja *puntocom*, debemos acudir de nuevo a la imagen del conflicto entre los que con una óptica comercial sobrevaloraron una versión de la web como una versión si intermediario de un centro comercial. La disrupción del nuevo medio, crecería en los márgenes dejados por esta crisis. En esta nueva selva de contenidos no dirigidos, creados por una comunidad cada vez mayor sin control central ni identidad más allá de la libertad de escritura, un buscador eficaz, apoyado por una publicidad sutil y no demasiado intrusiva se convertirá desde este origen práctico y modesto, en la pieza clave de toda la primera década de nuestro siglo[224].

---

[223] 4. Dans, E. *Todo va a cambiar*. Deusto. Madrid. 2010

[224] 5. Kleim, N. *No logo. El poder de las marcas*. Booket. Madrid. 2011

La Blogósfera

La Blogósfera, el mundo de los Blogs independientes y los conglomerados de estos, será hijo de este tiempo. Las primeras formas de blogs, alojados en hospedajes gratuitos como Geocities, nacían con una vocación totalmente diferente. En parte es la misma cultura que daría origen a la Wikipedia y otros proyectos de software libre. La revolución del blog, dejaría desconcertados a los grandes productores culturales, que asistirán a este fenómeno con una perplejidad de la que todavía no se han recuperado muchos de los grandes medios de comunicación, sobre todo en el entorno editorial. Tratar de cerrar el paso al avance de las bitácoras, con la traslación del medio escrito a la red, tratando de mantener la misma relación con el público que en los tiempos de papel llevarán al fracaso de las suscripciones del diarios como El País y El mundo, que en ambos casos renunciarían al modelo de suscripción en un periodo no muy dilatado en el tiempo a la luz del pobre resultado obtenido[225].

El resorte definitivo para la profesionalización de muchos de estos blogs vendrá de la mano de su principal beneficiario, Google. La inclusión de anuncios menos molestos, hasta cierto punto sutiles y ubicados en los márgenes del cuerpo de los blogs, en contraste con la verbena desconcertante de muchos de los portales generalistas, hará que *Adwords* triunfe como plataforma, durante muchos años casi en exclusiva, de publicidad. De esta simbiosis, surgirán muchos blogs profesionalizados y

[225] 6. Echeverría, J.: *Los Señores del aire: Telépolis y el Tercer Entorno*. Barcelona (Destino) 1999

cada vez de más amplia temática, para un internauta cada vez con menor perfil técnico y conocimiento del medio[226].

La nueva red es también heredera cultural del movimiento *underground* y del *ciberpunk*, muy vinculado a un subgénero literario de la denominada "ciencia ficción Dura" (Hard science fiction) en el que figuras como William Gibson, con su "*neuromante*"[227] o Neal Stephenson con "Snow Crash"[228] se adelantarán a los mundos futuros en los que la conexión es personal y portable y la red es un mundo paralelo en el que sumergirse en una inmersión completa. En 1999 saldrá a la luz el film "Matrix" de los hermanos Wachowsky y muchos de estos conceptos se popularizarán hasta el punto de condicionar el enfoque de futuros desarrollos de la red[229]. Los primeros movimientos de hactivismo con un foco político también compartirán época[230]. De hecho, el término "hacktivista" suele atribuirse al miembro del grupo de hackers *Cult of the Dead Cow* (CdC), llamado "*Omega*" y las actividades promovidas por este[231]. En España, diversos grupos de hackers comienzan a organizarse también en movimientos con objetivos más amplios que la investigación y el hacking. Fronteras Electrónicas España (FrEE)[232], un grupo surgido en

---

[226] La plataforma de publicidad de Google Adwords, es la clave en el negocio de Google*:* https://www.*google*.es/*adwords/*

[227] Gibson*, W. Neuromancer.* Minotauro. Barcelona.1989

[228] Stephenson*,* N.*Snow crash*. Gigamesh. Barcelona. 2008

[229] El film resultaría toda una referencia estética de su tiempo. La aparición de herramientas reales como *Nmap* para rastrear ip de usuarios no solo será un guiño a la comunidad hacker y ciberpunk sino que será una de las pocas ocasiones donde se empleen elementos reales para establecer una narrativa de ciencia ficción dura.

[230] 11. Mitnick, K.D. *El Arte de la Intrusión*. Ra-Ma. Madrid. 2006

[231] *Cult of the Dead Cow* sigue manteniendo presencia en la red:http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html

[232] Sobre Fronteras Electrónicas España. http://hackstory.net/FrEE

1996 y aliado del grupo EFF (Electronic Frontier Foundation) (13) norteamericano, mantendría una fuerte actividad, llegando a formar parte invitada por la comisión de Internet del Senado de España en 1998, momento en que con otras organizaciones promovieran la primera huelga de Internet, que se repetirá al año siguiente[233] Esta subcultura superficiará en organizaciones como Nodo50[234], que da soporte y alojamiento a diversos colectivos activistas desde 1994 o la Asociación de Internautas, activa hasta nuestros días[235].

También es el tiempo de Napster, y la descarga de música y contenidos de Internet. Con la extensión de las conexiones las redes de descargas comienzan a funcionar y los contenidos circulan como nunca loa habían hecho antes. Los sucesivos ataques a diferentes portales y formatos de compartir archivos tan solo harán mejorar la tecnología de estos. Pronto *Emule* y los enlaces *edk*, se generalizarán. Las redes de pares nacen con un espíritu ambivalente, entre los que buscan contenidos para consumirlos y los que ven en esta forma de compartir una manera de establecer comunidades[236]. De hecho, en España muchas de las páginas de recopilación de enlaces sobre temas específicos no tenían siquiera alternativa comercial viable, como en las primeras páginas literarias o dedicadas a ciertos tipos de música, o el recientemente desaparecido portal

---

[233] Sobre la primera Huelga de Internet en España y sus consecuencias: http://www.internautas.org/acciones/huelga6699/convo.html

[234] http://info.nodo50.org/

[235] .http://www.internautas.org/

[236] Molist, M. Hackstory.es. *Las historia nunca contada del underground hacker en la península ibérica.* 2014. Disponible en formato electrónico en*:* http://hackstory.es/

de subtitulado de contenidos substítulos.es[237], que ha cerrado su servicio el 1 de Julio de 2015, ante el temor del último cambio legislativo.

¿Burbuja 2.0?

Cuando expliquemos la expansión de las comunicaciones y el crecimiento de la web desde finales de la primera década de nuevo siglo hasta nuestros días, veremos los elementos principales sobre los que se apoya esta nueva escalada bursátil de compañías con modelos de negocio en algunos casos poco desarrollados o que se encuentran en proceso de comenzar a monetarizar la inversión. Esto resulta de especial interés para reconocer las diferencias de la escalada apreciativa de muchas empresas de la presente década respecto a la anterior burbuja. Así, a pesar de las fuertes apuestas y el continuo riesgo, veremos como la base de muchas de las grandes empresas si se sustancia en esta ocasión sobre modelos de negocio económicamente viables.

La primera década del siglo asistirá a la expansión y el predomino de Google como la gran empresa que ocupará buena parte de los nichos de mercado de Internet. Sin embargo, las redes sociales prosperarán al margen del control de esta empresa a pesar de varios intentos, como *Orkuc* (que tendría especial peso en Brasil), Google Wave, o Google Plus, la última apuesta que se llevaría por delante al lector de noticias RSS Google Reader, con una reacción contraria de una comunidad que hasta el momento simpatizaba con la política de la

[237] La primera baja de la denominada Ley Mordaza será un servicio único no ofrecido comercialmente que deja un nicho vacío en la red de servicios: http://www.eldiario.es/cultura/series/Primera-baja-Ley-Mordaza-subtituloses_0_403860432.html

empresa. Así compañías como Twitter, Linkedin o Facebook, que nacerían impulsadas por empresas de capital riesgo, que apostaban por ellas incluso antes de definir claramente su modelo de negocio, concurrirán en bolsa desde 2011 con capitalizaciones de nuevo muy elevadas. En concreto Linkedin, inicialmente una red profesional de intercambio de currículums profesionales, saldría por una capitalización de 7.800 millones de dólares y una acción valorada en 45 dólares; cifras que contrastaban con unos ingresos anuales de 161 millones y unos beneficios declarados de 10 millones[238] .

Sin embargo el caso de Facebook, será el más espectacular, al salir el 18 de mayo de 2012, casi ocho años después de su creación, debutando en la Bolsa Neoyorquina con un valor superior a los 100.000 millones de dólares. Este valor exorbitado si atendemos a sus cifras de negocio del momento, con unos ingresos de 3.700 millones y unos beneficios declarados de 1.000 millones, solo podía explicarse por un afán especulativo[239]. Aunque la empresa, con una liquidez de tal dimensión, iniciaría una política de adquisiciones bastante discutida en su momento, como en el caso de la compra de *WhatsApp*, la colocará como otra de las grandes de Internet, con 845 millones de usuarios (superaría los 1.000 millones en 2014), una cifra tan grande que cualquier inserción publicitaria es capaz de un impacto superior al de cualquier medio a lo largo de toda la historia de la humanidad.

---

[238] Análisis de la salida a bolsa de tres grandes de Internet*:* http://www.genbeta.com/genbeta/la-salida-a-bolsa-de-tres-grandes-empresas-tecnologicas-google-linkedin-y-facebook

[239] Cifras de cotización de Facebook en el índice Nasdaq: http://www.nasdaq.com/symbol/fb/real-time

Atendiendo al momento en el que muchas de estas compañías de Internet acuden a una nueva oleada de financiación e inversión bursátil, precisamente en un contexto de crisis global en el que los inversores han amplificado sus rotaciones de capital será complicado apuntar a una nueva burbuja. Si bien es cierto el desfase de las cifras, también la implantación de estas empresas y la propia red no es la misma que entresiglos. Buena parte del tráfico de Internet pasa hoy en día por los servicios de estas compañías. Hoy es común que la gente confunda la barra de su navegador con la búsqueda de Google o se informe vía Twitter o Facebook, más incluso que por los medios traicionarles de prensa y televisión. En ese sentido, el sobrevaloramiento tiene más relación con la cantidad de público potencial al que son capaces de acceder y transformar en ingresos reales que a la inversión realizada en estas empresas. En este contexto, es significativo que en enero de 2016 las cuatro primeras compañías mundiales en capilatización bursátil fueran los gigantes de la tecnología e internet, Google, Apple, Microsotf y Amazon.

El poder financiero adquirido por estas compañías, les ha llevado, como ya hemos apuntado anteriormente a desincentivar la innovación, cambiándola por una carrera de adquisiciones de talento e innovación. Los denominados "*unicornios*", compañías que entran en nichos de mercado nuevo, financiadas mediante "capital riesgo" y que ya superan los mil millones de dólares de valoración, entran en este juego apostando por medrar allí donde los "*dinosaurios*" no han sabido apuntar a tiempo[240]. La carrera entre la innovación y la adquisición de las grandes, que han colmado las fuentes de innovación de hace una década, deja a compañías *como Airbnb, Dropbox, Pinterest, Snapchat* o *Uber* en una

[240] Sobre los "unicornios" y la innovación de empresas disruptivas:http://www.enriquedans.com/2015/04/entre-unicornios-y-burbujas.html

posición compleja. Si bien es cierto que la adquisición de la competencia ha sido una constante entre estas grandes, también es cierto que estas pueden resistir y medrar en su mercado. Analizar el impulso de los inversores de capital riesgo en busca de rotaciones de capitales ascendentes puede explicarnos este juego de equilibrios en los que siempre hay que encaminarse hacia la apuesta más alta y que detenerse es asomarse al abismo[241] .

Mientras tanto, comunidades de usuarios y activistas de libertades cívicas siguen advirtiendo de los peligros de una red privatizada y dirigida por tan pocas compañías, de tan escasa transparencia y un interés cada vez más distante con las libertades individuales. Si bien es cierto que surgen alternativas de carácter libre y persisten “zonas de libertad" en algunos contextos, ahora mismo el mercado está ganando la partida de acaparar usuarios, en general acomodaticios y cada vez más espectadores de un momento histórico para las libertades[242]. La influencia y el control comercial de los medios digitales y las redes sociales y su sometimiento a los dictados de los gobiernos donde estas se radican y sus legislaciones poco transparentes en lo que respecta a la privacidad y los derechos nos sitúan ante una perspectiva ominosa, que exploraremos en detalle adelante, especialmente en el bloque cuarto.

---

[241] . Artículo de Fortune que detalla cómo son algunos de los denominados unicornios: http://fortune.com/2015/01/22/the-age-of-unicorns/

[242] Lessig.L. *Por una Cultura libre. Cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad*. LOM. Santiago, 2005. Edición electronica: http://www.traficantes.net/libros/por-una-cultura-libre

III: Mercado Virtual, Mediatización y Cultura Digital

3.1 Una sociedad en transformación constante

El cambio de paradigma, en sentidos múltiples, como hasta el momento hemos podido ver, ha supuesto la apertura de un debate sobre si se trata de un cambio del propio sistema mundial, en forma estructurada como la de define Wallernstein, o más bien de una reedición del mismo sistema capitalista bajo una remozada versión de liberalismo clásico, actualizado a la luz del avances tecnológicos[243]. Tal vez sea la pasión por el etiquetado lo que nos haga entrar en este tipo de debates que, en el fondo, definen los mismos parámetros, sin importar que sea evolución o transformación sino la descripción de los factores de cambio, los nuevos parámetros y las orientaciones que se toman. En este sentido, es cierto que estamos inmersos en una serie de diferencias respecto al contexto anterior al periodo reciente de este entresiglos, en el que han confluido una serie de factores que harán, cuando exista suficiente distancia temporal para poder observarlo de forma retrospectiva, que el contexto actual, que ha empezado ahora, sea netamente diferenciable del anterior a lo largo del siglo XX.

Efectivamente, hemos podido observar cómo paulatinamente, la sociedad en la que vivimos es diferente a la que pudimos conocer dos décadas antes. En este sentido, la tecnología, sin ser el factor absoluto, sí que ha sido un desencadenante de varios procesos, sobre todo en cuanto a la pronunciación de elementos que ya estaban prefijando en los aspectos económicos, como la integración de mercados, las nuevas formas de organización empresarial y el auge de unos mercados financieros que

[243] Wallernstein, I. *Geopolítica y Geocultura. Ensayos sobre el moderno sistema mundial.* Kairós, Barcelona, 2007.

actúan fuera de la ligazón concreta del sector productivo que teóricamente financian con su inversión [244]. La crisis de los modelos económicos precedentes, tanto del experimento socialista en el este de Europa (el caso Chino merecería mención aparte como capitalismo de estado) como el paradigma de Estado del bienestar, junto con el auge de un Pensamiento Único que ha apadrinado el proceso de globalización bajo la doctrina de liberalismo han sido elementos fundamentales en este proceso. Estos cambios suponen un cambio social profundo, con unas características nuevas, no solo por la exposición a una nueva forma de establecerse las relaciones laborales, sin garantías ni estabilidad como las conocidas hasta ahora, mayores diferencias sociales, con el incremento de los índices de exclusión social dentro de una competitividad extremada, que obliga al individuo al reciclaje continuo, so riesgo de caer del mercado laboral, sino también en la forma en que la propia sociedad se organiza.

Junto con esto, la sociedad se orienta hacia la red, mediante la implementación privada de herramientas propias de esta, aplicadas al ámbito del consumo. La mutación del *ciudadano* al *consumidor*/*espectador*[245], será uno de los fenómenos característicos de este periodo, acompañado por el mayor aislamiento social e individualismo, en los sectores integrados socialmente. Junto con esto, el desencanto por una actividad política, convergida ideológicamente bajo unos parámetros en esencia similares y movida por intereses cada vez más corporativos y menos determinantes en el aspecto económico, tras la efectiva renuncia a toda capacidad de intervención radical en el sistema, trasladará las inquietudes sociales en dos caminos diferenciados, casi paralelos al nivel

---

[244] Manuel Castells. *La era de la información: economía, sociedad y cultura (Vol. 3): La sociedad red. Fin del milenio*. Alianza editorial. Madrid. 2008

[245] Marc Augé. *Sobremodernidad: del mundo tecnológico de hoy al desafío esencial del mañana. En Sociedad Mediatizada*. Gedisa. Barcelona.2007

sociocultural; por una parte, en movimientos sociales que renuncian al poder como forma de intervención y buscan modificaciones concretas, como ecologistas, feministas y otros plataformas reivindicativas, y por otro lado, los de la parte más excluida de la sociedad o falta de referentes, que viven un auténtico auge de los valores que los movimientos anteriores considerarían superados como los nacionalismos o los fundamentalismos religiosos como referentes que acuden a lo grupal.

En términos sociales este último periodo ha adolecido de una indefinición en lo que respecta a referentes. Desde manifiestos como el Cluerain [246] que pretendían hacer al consumidor un sujeto activo en conversación constante con la vieja empresa pero plegado a la pose de la mitología de la nueva empresa, encarnada bajo el lema del *Dont be evi*l (no seas malo) de Google, en seria revisión durante la última década[247], hasta movimientos más activos como las primeras organizaciones antiglobalización de los 90' que con el tiempo emplearían asimismo herramientas sociales de la red hasta concretar movimientos internacionales con desigual impacto en las políticas nacionales e internacionales[248], se puede trazar un itinerario de avance lento y superado por las circunstancias y los ritmos impuestos por los auténticos agentes del cambio. Hasta el momento la fuerza y la capacidad de todos estos movimientos no han conseguido ser una respuesta suficiente a la doctrina neoliberal y su programa socioeconómico de uniformación a escala

---

[246] VVAA. Manifiesto Cluerain http://www.cluetrain.com/ Las tesis en castellano podemos encontrarlas en: http://tremendo.com/cluetrain/ . 1999.

[247] 5. Reischl, G. *El engaño de Google.* Medialive Content. Barcelona. 2008

[248] 6. VVAA. *Internet y Lucha política: Los movimientos sociales en la red*. Capital Intelectual, Buenos Aires, 2006

planetaria, aunque se han cosechado éxitos parciales y denuncias de impacto[249].

La profunda transformación que ha supuesto la crisis económica ha significado, en términos sociales, una aceleración de los principios neoliberales hasta límites que difícilmente habría tolerado una sociedad democrática durante la primera década del siglo. Esto es debido en parte al choque de las medidas[250] y el contexto previo a esta crisis, en los que los valores colectivos habían sido suficientemente mermados como para poder entablar los cambios sin grandes organizaciones civiles ni partidarias capaces de articular una gran respuesta social.

El propio concepto de crisis, de situación de constante emergencia, ha sido combustible suficiente para que una sociedad completa se someta a una doctrina sin poder organizar una crítica suficiente como para establecer una alternativa adecuada a un sistema que se reconoce incapaz de resolver sus propias contradicciones[251].

A lo largo de los dos bloques anteriores hemos visto cómo se ha organizado el poder económico y la expansión de una forma de gran empresa transnacional fundamentada en la capacidad de su red global. También hemos visto cómo se organiza Internet y se establecen las bases de lo que es hoy en día y hemos sugerido ámbitos de disputa entre formas de entender las libertades dentro de esta red. Como hemos señalado, por encima de la descripción, la tarea principal de nuestro trabajo es encontrar las fuentes y los elementos principales del conflicto en la

---

[249] 7. Echeverría, J.*: Los Señores del aire: Telépolis y el Tercer Entorno*. Barcelona (Destino) 1999

[250] 8. Kleim, N. *La doctrina del Shock. El auge del capitalismo del desastre*. Booket. Madrid. 2012

[251] 9. Lanier, J. *Contra el rebaño digital: Un manifiesto*. Debate. Barcelona. 2011

sociedad de la información y cómo Internet es su escenario principal, al ser el medio base sobre el que se está estructurando el camino de la sociedad actual. En los diferentes puntos del presente bloque, describiremos algunos de los elementos principales de la parte mercantil del conflicto, la legislación y cómo el mercado y resistencia de ciertos modelos obsoletos de negocio a adaptarse acaban en desastres legislativos y persecución de usuarios.

3.2 Intentos reglamentadores de la sociedad de la información

Como en los anteriores bloques señaláramos, el auge técnico y la capacidad de las telecomunicaciones vivieron un proceso paulatino de expansión, condicionando tanto por el propio soporte y las formas de interconexión como por la popularización de medios técnicos, sobre todo el ordenador personal en la primera etapa. A este respecto varias iniciativas de los diferentes estamentos posibilitarían este auge, como la fragmentación en EEUU de AT&T, y las diferentes aperturas del sector, así como el establecimiento de diversos protocolos estandarizados como base de las comunicaciones.

La desreglamentación de las telecomunicaciones y la inserción de estas como aspecto a tratar en acuerdos comerciales internacionales serán factores que nos indican como, desde un periodo bien temprano en la creación de la sociedad de la información. Curiosamente, uno de los primeros debates sobre el libre flujo de la información y la comunicación, se daría en el seno de la UNESCO en los años setenta, cuando se pretendió instaurar el denominado *Nuevo Orden Mundial de la Información y la Comunicación* (NOMIC)[252], impulsado principalmente por el grupo de países No alineados, con la preocupación respecto a cómo la información sería manejada a escala global, dada la creciente concentración a cargo de empresas extranjeras. Para tal fin, se establecería un plan para debatir y regular la información y comunicación, ante las carencias en cuanto a transparencia y libertad de prensa efectiva en buena parte del tercer mundo. El debate llegaría en 1976 a un punto álgido en la Asamblea

[252] Herrera León, B. *El modelo UNESCO de comunicación en el «Informe MacBride»*. Anuario Inicio, jun. 2005, vol.17, no.1

General de la UNESCO, dado por un lado la ausencia de interés por parte de ciertos estados, sobre todo de Gran Bretaña y Estados Unidos, a cuyas compañías no les interesaba tratar sobre los medios o la brecha digital y el núcleo principal de los No alineados, interesados en el debate[253]. La salida ha dicho bloqueo vendría por medio de la creación de la C*omisión Internacional para el Estudio de los Problemas de la Comunicación*, conocida como la Comisión MacBride debido al nombre de su presidente, Sean MacBride, premio Nobel de la Paz y cofundador de Amnistía Internacional.

Para la asamblea de 1980, presentaría su primer informe denominado *"Un solo mundo. Voces múltiples. Comunicación en información en nuestro tiempo"*[254], en el que se hacía hincapié en el proceso de concentración de las comunicaciones y las contradicciones y problemas que esto entrañaba, lo que, a pesar a eludir la exposición directa de ciertas cuestiones, sí que establecía 82 recomendaciones concretas, bajo la perspectiva de cómo la evolución del proceso técnico incidiría en las comunicaciones y la información, para avanzar en propuestas acerca de la democratización y el acceso en igualdad de condiciones de todos los agentes en favor de un equilibrio internacional con los derechos humanos como principal orientación de todas estas medidas. Finalmente, se conseguiría llegar a un consenso que, bajo el concepto del "derecho a comunicar", auténtico *leitmotiv* del informe, unificaría las posiciones mayoritarias de la asamblea, lo que no significaría su puesta en práctica,

---

253 Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

254 McBride y otros. *Un solo mundo. Voces múltiples. Comunicación en información en nuestro tiempo.* Fondo de Cultura Económica y UNESCO. México, 1980. Disponible en: http Disponible en: http://unesdoc.unesco.org/images/0004/000400/040066sb.pdf

dada la completa oposición de corporaciones y gobiernos concretos, con el caso del estadounidense como su principal contrincante.

La llegada al poder de Reagan, pondría en perspectiva la intencionalidad de los agentes opuestos a estos acuerdos, consiguiendo finalmente que el propio organismo de las Naciones Unidas quedara en una posición residual dentro de la política internacional de comunicaciones, derivadas, como veremos, a lo comercial. El principal argumentario empleado en esta ofensiva sería precisamente la defensa de las libertades de prensa frente a países, entre los que habían aprobado el informe, que trataban de imponer el control gubernamental sobre los medios de comunicación, terminando por acusar al proyecto de McBride de "sovietizante", excusa para desligarse de la UNESCO. El fin oficial del organismo, llegaría en 1989, bajo el mandato de Federico Mayor Zaragoza, con la adopción de la denominada *"Nueva Estrategia de la Comunicación*", mientras los debates de McBride continuarían a cargo de ONG y otros organismos a modo de mesa redonda otra década más, fuera de la UNESCO. Uno de los legados más importantes de esta tentativa sería la puesta en debate de un tema fundamental para la sociedad de la información en proceso, las nuevas tecnologías de la información y la comunicación necesitaban mecanismos de control fuera del interés mercantilista de las grandes empresas y los gobiernos que las respaldan. En contraposición, la doctrina que establece la información y comunicación como "nuevo recurso nacional", teorizado por primera vez en 1977, en el informe titulado, *The New World Information Order*, sienta las bases doctrinarias de un desarrollo "sin reservas ni condiciones" que confrontaran con este enfoque. La realidad es que la posición dominante en todos los desarrollos relativos a la sociedad de la información por parte de empresas estratégicas de EEUU y sus aliados más directos le permiten ejercer una posición de fuerza y ruptura de consenso que es condición para cualquier resolución en la práctica.

Desreglamentación empresarial y datos personales

El proceso de desreglamentación de las telecomunicaciones viene de la mano del ascenso del ideario neoliberal, tanto en los Estados Unidos, como en Europa, a través de sus sucesivas instituciones, y los organismos internacionales, desde el estreno del término "sociedad de la Información" por parte de la OCDE, en una de sus cumbres de 1975. Poco después, la entonces Comunidad Económica Europea, adopta la noción para un programa quinquenal denominado FAST (Forecasting and Assessment in the field of Science and Technology)[255] a través del que pretenderá establecer una evaluación y prospectiva sobre las nuevas tecnologías y su impacto social. Otros organismos internacionales mostrarán su preocupación sobre el impacto de las nuevas tecnologías y la informatización en el empleo, como la OIT y diversas confederaciones sindicales. Los temores por la disposición y el manejo de datos personales llevarán a la Comisión Europea a la redacción, en 1980, de un "convenio para la protección de las personas con relación al tratamiento automatizado de datos de carácter personal", contando como principal prerrogativa la capacidad de disponer de sus datos de cualquier persona física. El mismo año, la OCDE, adoptará una recomendación respecto al flujo internacional de datos personales.

A partir de ese momento el proceso de reglamentación de los datos personales irá en paralelo al de la desreglamentación de las

[255] El memorándum se encuentra disponble en: The FAST programme - forecasting and assessment in the field of science and technology. Information Memo P-29/80, April 1980 http://aei.pitt.edu/31042/

telecomunicaciones mismas, en manos de organismos de carácter económico, como los propios documentos citados exponen, al remarcar en su redacción que los estados deberían abstenerse de reglamentaciones sobre el tratamiento de datos que llegaran a obstaculizar la libre circulación de datos de carácter personal, lo que ubica el carácter de estas iniciativas y los límites que en ellas mismas se colocan. La presión por parte de organismos sociales y otras organizaciones, ante la amenaza de un tratamiento de esos datos por parte de empresas privadas, llevará finalmente a una nueva redacción, en 1998, de una Directiva Europea sobre la protección de datos personales[256], de la que la L*ey sobre la protección de datos* española, del siguiente año, será una derivación subsecuente[257], junto con la misma Agencia Española de Protección de Datos[258]. Esta iniciativa provocará las protestas de las autoridades norteamericanas, de donde provienen la mayor parte de compañías que atesoran datos personales de ciudadanos europeos, bajo la acusación de entorpecer el comercio electrónico. De cualquier modo, serán precisamente estas compañías la que continuarán integrando datos que rastrean el paso de los usuarios por diversas aplicaciones *en línea*, como AOL, Microsoft, Google, Myspace o Facebook, precisamente con cláusulas que en muchos casos vulneran este nuevo entorno legal, so pretexto de la voluntariedad de los

[256] La directiva, recientemente reeditada y en proceso abierto de nueva redacción a lo largo de 2015 y especialmente tras las nuevas negociaciones bilaterales respecto a Privacy Shield con EEUU, acerca del tratamiento y cesión de datos entre partes, se encutra disponible en http://ec.europa.eu/justice/data-protection/index_es.htm. Su reforma, que se encutra en proceso de redacción y acuerdo en 2016 puede ser consultada en: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[257] Ley orgánica 15/99 sobre la protección de datos de carácter personal. https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/Ley-15_99.pdf

[258] Agencia española de protección de datos: https://www.agpd.es

usuarios en ceder los datos personales o la persistencia de estos datos para favorecer motores de búsqueda[259].

A partir del *Patriot Act*[260], producto directo de los atentados del 11 de septiembre de 2001 en EEUU, el tratamiento legal de datos de personas por parte de este estado será regulado de forma más severa y con un alcance internacional, al margen de cualquier acuerdo. Como veremos especialmente en el bloque cuarto de nuestro trabajo, esta política llevara no solo a una colisión de intereses entre estados sino entre empresas y muchos principios democráticos, sacrificados en aras de un concepto de seguridad cada vez más amplio e impreciso.

Continuando con el proceso de expansión de las telecomunicaciones, señalaremos cómo este irá en paralelo a su liberalización y la desreglamentación de todos los mecanismos estatales de control o tutela, como hemos señalado, de la mano de grandes privatizaciones, como la que el gobierno Thatcher realizara de BT (British Telecom) o el desmantelamiento del gran monopolio estadounidense de la AT&T, ambos procesos finalizados a lo largo de 1984. Una de las consecuencias de esto será la existencia de grandes empresas de telecomunicaciones surgidas a partir de anteriores conglomerados públicos, en situación dominante cuando no directamente monopolista. El caso de *Telefónica*, en España, es paradigma de ello. Una vez privatizada, con un mercado de origen completamente dominado y una ingente capitalización, podrá expandirse con una posición inicial de fuerza que la

---

[259] Preuss-Laussionotte, S. *La democracia ante los riesgos de la mundialización de las bases de datos*. En El estado del mundo 2009. Akal, Barcelona 2008.

[260] Enlace protegido de borrados a la USA Patriot Act: http://web.archive.org/web/http://www.lifeandliberty.gov/highlights.htm

llevará a convertirse en una de las empresas líderes del sector a escala internacional.

De forma paralela el avance de un gran acuerdo en el marco de la OMC (Organización Mundial del Comercio)[261], firmado por setenta y ocho gobiernos, sobre la apertura de los mercados de telecomunicaciones a la competencia, posibilitará que a partir de 1998, se lleve a cabo un proceso acelerado e irreversible de ampliación de la capacidad de influencia, inversión y penetración de grandes compañías en el mercado mundial. La ventaja comparativa de partir de sectores con grandes mercados prácticamente exclusivos y cuentas de resultados ya de partida con grandes beneficios empujará un proceso de fusiones y acuerdos que dará lugar a un gran conglomerado de monopolios o grandes trust del sector, que dispondrán del mercado del sector enfrentados a un constante proceso legal para evadir cualquier intento de acotar a esos monopolios de hecho[262].

Como hemos visto, tanto este acuerdo, como las políticas nacionales de apertura de mercados y privatización de servicios llevaran a la expansión de las grandes empresas de telecomunicaciones. El proceso de grandes privatizaciones de sectores estratégicos bajo tutela estatal hasta entonces y más especialmente en este sector, permitirá esta fase expansionista. Sin embargo, salvo el desarrollo e implantación de nuevas tecnologías en cuanto al proceso físico, ninguna de estas grandes empresas del sector sabrán posicionarse en el medio al que dan soporte. La gran capitalización de estas y la capacidad de compra y expansión no será sin embargo un

---

[261] OCM: https://www.wto.org/indexsp.htm

[262] Manuel Castells. *La era de la información: economía, sociedad y cultura (Vol. 1): La sociedad red.* Alianza editorial. Madrid. 2008

factor que les otorgue el dominio inmediato de la red que bajo su infraestructura se estaba expandiendo. Como veremos, la posición de dominio pudo en su momento impedirles ver que los nuevos negocios que se fraguaban en la red no seguían el patrón que podían esperarse. El servicio más que la tecnología que da soporte será el gran pilar de la expansión posterior a la crisis de las *puntocom*.

El precio de la expansión en el contexto de la globalización

Todo el proceso expansivo que viven las grandes compañías del sector tecnológico y las comunicaciones parte de un origen ideológico identificado con la doctrina neoliberal en el plano económico, aunque con una férrea tutela identificada con el auge *Neocon* (nuevo conservadurismo identificado con el *Tea Party* norteamericano y grupos de la derecha europea) en lo que respecta a derechos civiles y control democrático del medio. Frente a esta política, en la que cada ronda negociadora suponía una vuelta de tuerca a favor de la gran empresa, no se organizará ningún modelo de respuesta a gran escala hasta que, para la nueva cumbre de la OMC, que se celebrara en noviembre de 1999 en la localidad norteamericana de Seattle, múltiples organizaciones, entorno a movimientos *antiglobalización*, organizarán una gran protesta, conocida desde entonces como *la Batalla de Seattle*[263]. A partir de ese episodio de respuesta cívica, diversas organizaciones antiglobalización pondrán el foco en los aspectos menos democráticos de estas negociaciones, en buena

[263] 14. AAVV. *Internet y lucha política. Los movimientos sociales en la red*. Capital Intelectual, Buenos Aires, 2006

medida hurtadas del debate democrático en parlamentos y apenas trasladada en los medios a un auténtico debate ciudadano acerca de qué intereses defendían estos acuerdos[264].

A partir de este hito, comenzará la organización de puntos de encuentro de activistas a escala internacional para fijar una respuesta y debate común sobre este tipo de acuerdos internacionales. La organización del Foro Social Mundial, el primero de ellos en la ciudad brasileña de Porto Alegre, para articular una primera respuesta a la doctrina neoliberal promulgada de forma unívoca por la OCM y otros organismos internacionales como el Banco Mundial O el FMI. La mayor crítica que este encuentro de activistas es la de constatar que estos organismos actúan como agentes que tratan de coaccionar la política económica de todos los países que entran en su órbita para que adopten la doctrina económica que favorece los intereses de los poderosos, sin ningún objetivo social que no sea el de la desregulación de mercados para potenciar el dominio de la gran empresa[265].

A pesar de dichas propuestas, que comienzan a organizar una respuesta global, las más de las veces al margen de organizaciones partidarias, por tanto fuera del ámbito de decisión política efectiva, el auge de la "nueva economía" se conformará como un proceso irreversible, precisamente por el condicionamiento económico que imposibilita a los estados, en caso de desearlo, cuestionar o salir de dicho proceso

---

[264] Un trabajo de recopilación de primer orden a cargo de un grupo de investigación de la Universidad de Washington contene una de las mejores fuentes actuales sobre los acontecimentos en torno a la cumbre de la OCM y la contracumbre: http://depts.washington.edu/wtohist/index.htm

[265] Docuemnto del FMI sobre la ruta económica que pretende trazar para la economía mundial. *La globalización ¿amenaza u oportunidad?* : http://www.imf.org/external/np/exr/ib/2000/esl/041200s.htm

económico. De este modo, veremos en primer lugar cómo la burbuja de las denominadas a principios de siglo *"puntocom",* compañías que señalamos que operan principalmente en la red, se irá imbricando rápidamente en la economía global, con adquisiciones espectaculares. Entre los casos mas destacados podemos señalar el de la operadora de telecomunicaciones AOL con la adquisición del grupo mediático Time-Warner, o la entrada de Microsoft en la televisión convencional con la adquisición de la NBC[266]. Este proceso continuará permeando a lo largo de diversos sectores, especialmente tras el repliegue de lo público.

La *Global Information Infraestructure*, será otro organismo, impulsado por el entonces vicepresidente norteamericano del Gobierno Clinton, Al Gore, que tratará, bajo el supuesto intento de evangelización tecnológica, previo pago de la asunción incuestionable de la doctrina económica y política fijada por el FMI y el BM, de dar un aspecto progresista al proceso, con afirmaciones como que *"la maraña inconsútil de redes de comunicación, ordenadores, bases de datos y electrónica de consumo que ofrecerán a los usuarios ingentes cantidades de información al alcance de sus manos*"[267]. La propia Unión Europea, en el informe del comisario Bangeman, de 1994, titulado *Europa y la sociedad de la información planetaria*, tratará de teorizar al respecto, demostrando una doctrina similar a la de Gore, al afirmar que la liberalización favoreceré la difusión de las comunicaciones globales y el acceso al conocimiento, bajo la premisa que en una sociedad donde el trabajo y el capital ya no son las variables

---

[266] Bustamante, E. *Hacia un nuevo sistema mundial de comunicación: las industrias culturales de la era digital.* Gedisa, Barcelona, 2004

[267] 18. Ramonet, I. *"Nouveau pretê-á-penser ideologique*". Le Monde Diplomatique, Mayo- 1992

centrales de la economía sino esta información y conocimiento, entendidas como producto comercial cuya circulación se debe favorecer, deplorando cualquier proceso de limitación de este, entre los que la libertad de expresión podría deducirse[268]. Nuevas reuniones de dicho organismo, junto con otro informe similar, denominado *Libro Verde sobre las telecomunicaciones*, encargado de nuevo al comisario Bangeman[269], poco antes de que se desatara el escándalo acerca de su fichaje por Telefónica, después de ser favorecida por este, abundarán en esa intención de dar respaldo a la liberalización completa del sector, confirmada después en una nueva cumbre del G-7, con propuestas de "aligeramiento" reglamentario del sector.

En el caso europeo, el proceso de unificación de mercados y moneda, no supondrá más que un avance en los diseños prefijados respecto a la Información y la comunicación, que curiosamente, en ningún aspecto cuestionan las patentes o los derechos de autor, en favor de las compañías que atesora esta información en beneficio propio, a pesar de la implacable liberalización que se preconiza, como quedará patente en la Cumbre Económica y Social celebrada en Lisboa en 2000.

Como hemos podido ver, al margen de declaraciones de intenciones y discursos vacuos, la dirección de todo el proceso de acuerdos y legislaciones abundará en la intención de potenciar una desregulación del sector de las comunicaciones y amparar los intereses de los grandes grupos ya ubicados en este. Buena parte de las contradicciones expresadas en estos acuerdos, mayoritariamente a puerta cerrada y

---

[268] 19. Materland, A. *La información contra el estado*. Le Monde Diplomatique, nº 21 Marzo 2001

[269] 20. Comisión europea. *Green Paper. Living and Working in the Information Society: People First.* Disponible en: http.//www.hamburg.de/ English/StadtPol/Europe/peopl1st.htm

conocidos por sucesivas filtraciones, se pondrán de manifiesto al defender en ciertos casos modelos de negocio, sobre todo en lo referente a derechos de autor y difusión de medios audiovisuales. Acuerdos como el ACTA (Anti-Counterfeiting Trade Agreement), finalmente rechazados por la UE, una vez filtrados los textos puestos a debate, significará una declaración de los principios, de la hoja de ruta del neoliberalismo, en el sector de las telecomunicaciones e Internet. Recurrentemente, supuestos acuerdos comerciales bilaterales, principalmente entre EEUU y la UE, como TAFTA (Trans-Atlantic Free Trade Agreement) o CETA (Canadá-EU Trade Agreement), volverán a poner sobre la mesa la supresión del derecho nacional sobre grandes compañías o la exención de control fiscal o laboral de estas, entre otros apartados[270]. Sin embargo, resulta curioso cómo estos acuerdos, de un modo u otro apuntaban de forma recurrente en cuestiones como los derechos de autor, la propiedad intelectual y la piratería con un endurecimiento legal y una persecución que en algunos casos sugería una vulneración de los derechos ciudadanos[271].

Por otra parte, compañías del sector han querido aprovechar la oportunidad de estos tratados para cuestionar la neutralidad de la red, tanto desde el punto de vista comercial, ofreciendo Internet a diferentes velocidades dependiendo de los productos y servicios de los que se hagan uso como mediante el control de la conexión y su tráfico[272]. Precisamente la

---

[270] La ONG *La Cuadrature du Net,* ha sido uno de los agentes más activos en contra de este proceso y cuenta con grandes dosieres sobre cada uno de estos acuerdos. Sobre ACTA: http://www.laquadrature.net/en/ACTA ; Sobre CETA: http://www.laquadrature.net/en/CETA y sobre TAFTA: http://www.laquadrature.net/en/TAFTA

[271] Sobre TAFTA, existe extensa documentación. En su momento, redacté un resumen de sus puntos más destacados: TAFTA: La crisis como excusa para volver a intentar restringir libertades en: http://www.eldiario.es/turing/Comision-Europea-intentar-restringir-libertades_0_123188473.html

[272] Una de las explicaciones más recientes sobre la importancia de la neutralidad de la red nos la ofrece la ONG EDRI: https://edri.org/net-neutrality-in-critical-danger/

posición dominante de muchas compañías estadounidenses que operan en la red hizo que el debate sobre CISPA (Cyber Intelligence Sharing and Protection Act), una legislación que permitía el espionaje de las comunicaciones sin restricciones, legalizando buena parte de los aspectos más discutibles de la *Patriot Act,* tuviese tanta relevancia internacional. Junto a ello, la revelación de las peticiones de datos a grandes empresas de la red sobre sus usuarios por parte del gobierno norteamericano y las revelaciones de WikiLeaks sobre la colaboración y la resistencia parcial de algunas de estas compañías, como Twitter, en esta puesta a disposición de datos personales, no siempre con orden judicial, colocaron el debate en un primer plano que destacaría mas si cabe la transcendencia de dichas negociaciones[273].

A lo largo de 2015, el TTIP, la décima ronda de negociación del antes denominado como TAFTA recupera buena parte del argumentario de algunos intentos previos, como ACTA, en temas de propiedad intelectual y patentado de software, con tribunales de arbitraje especiales para las grandes transnacionales, que escapan así del control judicial de cada estado, junto con la "liberalización" de sectores como la salud o la gestión de aguas y una mayor desregulación del marco de relaciones laborales y salariales. En esencia el acuerdo es un calco del TPP, que se negocia en el ámbito del pacífico[274]. La forma en la que se enfoca esta nueva oleada

---

[273] Debido a mi actividad en ciertos medios del sector, también compuse un artículo explicando el debate sobre CISPA, su relevancia y el impacto posible de sus medidas respecto a libertades cuidadanas en la red:.http://www.eldiario.es/turing/aprobacion-CISPA-legalizara-espionaje-ciudadano_0_122837866.html

[274] Sobre el TPP, que por no afectar directamente a Europa ha sido un asunto sobre el que no se ha prestado suficiente atención, a pesar de ser un calco del TIPP, también realizaría un apunte sobre el asunto durante la celebración de una de sus más recientes rondas: *TPP: Una negociación diseñada para favorecer intereses lobistas*: http://www.eldiario.es/turing/TPP-negociacion-favorecer-intereses-lobistas_0_137536755.html

de acuerdos multilaterales, sin debate incluso dentro de los parlamentos de los estados afectados y con las mismos pautas en diversos escenarios nos muestran un diseño común, que parte de los mismos intereses. Como vemos, el tema deriva en la actualidad del preciso momento en el que redactamos el presente trabajo pero tanto la dirección como la intención se encontraban ampliamente prefijados. A lo largo del Bloque siguiente se ahondara en los aspectos de derechos de autor, cibervigilancia y filtraciones, con lo que el contexto presente de las negociaciones abiertas quedará fijado.

3.3 La nueva dimensión del Big Data

La denominación Big Data es un tema de gran actualidad, que hace referencia a manejo de grandes cantidades de datos que requieren de una infraestructura informática de envergadura suficiente para poder enfrentarlas y extraer datos de interés. El perfil de las empresas y organismos hacen uso del Big Data resulta muy variado, desde el mismo CERN, en su Gran Acelerador de Hadrones[275], para la recolección masiva de los datos generados en su proceso experimental, hasta el análisis financiero, pasando la recolección de perfiles sociales de los que destilar pautas para su empleo publicitario. En todos los casos, se requieren máquinas de gran procesado de datos capaces de ofrecer pautas y localizar patrones así como separar conjuntos de estos y establecer modelos de visualización capaces de ser interpretados por un humano[276].

El término comenzó a popularizarse a principios del presente siglo, cuando se hacía evidente la necesidad de un uso de cada vez mayor cantidad de datos que deben ser filtrados y catalogados de un modo que los haga manejables para poder hacer un uso adecuado de ellos. Como asegurase Doug Laney[277], analista de datos, en 2001, el Big Data puede

---

[275] CERN: El empleo de datos masivos por parte del Gran Colisionador de Hadrones es parte fundamental en la interpretación de unos datos que son tomados en cuestión de fracciones de segundos pero en una cantidad ingente. http://home.web.cern.ch/topics/large-hadron-collider

[276] . IBM ofrece un manual de interpretación del Big Data con cifras y estadísticas muy interesante*: Big Data Beyond the Hype: A Guide to Conversations for Today's Data Center*, disponible en: https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=ibm-analytics&S_PKG=ov28197&S_TACT=M161001W&dynform=11707&lang=en_US

[277] El Documento donde Doug Laney, explica cómo se organiza el Big Data se encuentra disponible en:http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

ser definido con las tres "V" (Volumen, Velocidad y Variedad). En realidad, en su definición nos indica cómo la industria comienza a ver la forma en la que va e evolucionar la cantidad de información disponible y cómo esta se convierte en un elemento crítico en su negocio. Aunque en los aspectos más sociales guarde una relación directa con la estadística, la forma en la que se enfrenta la información obtenida y el resultado son distintos.

A la mayor parte de las grandes compañías de telecomunicaciones y empresas que operan en Internet les resultaría imposible mantener su negocio sin el manejo correcto de la gran cantidad de datos que circulan a diario por sus servidores. Proyectos de carácter científicos como el del Genoma humano [278] habrían sido imposibles sin las herramientas de procesado de datos adquiridos. En la actualidad, el periodismo de datos y el análisis financiero se han convertido en empleos que hace uso de estas grandes recopilaciones de datos. La capacidad de manejar estos datos ofrece una ventaja competitiva y por tanto es uno de los nuevos frentes de los departamentos de Investigación y expansión de grandes empresas. Anteriormente, citamos el modelo de negocio de la empresa identificada con la nueva economía y nombramos el ejemplo de compañías como Zara y su formato de adecuación de oferta por tienda a tiempo de cierre de cada uno de sus establecimientos. Esta capacidad sería imposible sin elementos de análisis estadísticos capaces de cubrir todo el rango de su negocio[279].

Cada vez son más los proyectos que hacen uso de cantidades de datos de mayor complejidad. A lo largo de los anteriores capítulos del

[278] Proyecto genoma humano: www.sciencemag.org/content/291/5507/1218.full

[279] informe de CISCO sobre el impacto de la inversión en TI y Big data en la empresa: http://www.cisco.com/web/ES/about/press/2013/2013-04-02-big-data-gran-potencial-y-prioridad-de-negocio.html

presente trabajo podemos deducir cómo esta gestión de datos, es parte basal del negocio de la nueva empresa orientada a la red, la conexión y el procesado de esta nueva "materia" de negocio, el dato, es el nuevo elemento de riqueza[280]. El papel de los usuarios y consumidores en este proceso es fundamental y por ello podemos explicarnos la cantidad de servicios gratuitos que han acompañado al periodo de mayor expansión de la red. Los datos personales son el eje de buena parte del negocio digital, el centro mismo de la economía basada en la sociedad de la información, por ello el tránsito de unos servicios de peaje a un modelo de *socialización* y gratuidad, han corrido en paralelo al valor del dato personal como moneda de cambio.

Ya resulta un tópico la afirmación de que cuando no hay modelo de negocio es el usuario el negocio, pero el avance en la captación de cada vez mayor cantidad de datos de carácter personal por parte de compañías que basan su negocio principalmente en la publicidad, como Facebook o Google, no deja margen para negarlo. El modelo de esta última, se puede rastrear mediante la reacción al bloqueo en la captación de datos. Tanto en los navegadores, con su "acuerdo" con *Adblock* (un potente bloqueador de publicidad para navegador), para que "deje pasar" ciertos anuncios de su "lista blanca"[281], como respecto al propio Android, con la reacción frente a desarrollos como CyanogenMod[282], que prescinden de la tienda y las aplicaciones de la gran G, ha quedado patente que la gratuidad de sus servicios se fundamenta en la exposición del usuario a permitir el tratamiento de sus datos de cada vez mayor diversidad de formas.

---

[280] Al respecto del valor de los datos como nueva mercancía compuse un artículo para eldiario.es que resume buena parte de los aspectos aquí tratados: Big Data y la privacidad: Cuando el negocio eres tú: http://www.eldiario.es/turing/BigData_0_120038458.html

[281] 7. Adblock, el bloqueador de anuncios "amigo de Google": https://getadblock.com/

[282] . CyanogenMod, uno de los desarrollos de Android paralelos más afamados: http://www.cyanogenmod.org/

Las bases de datos como eje del procesado de información

En la era de la información ya hemos visto cómo ser dominante en un negocio tan solo puede otorgar a la empresa en cuestión una mejor posición de partida. No adaptarse supone quedar desplazado de las constantes oleadas que sacuden a las empresas de Internet. En este marco Oracle [283] era hegemónica en principio y ofrecía su paquete de servidores de datos a grandes empresas con un modelo de gestión de clientes y recursos estructurado pero no focalizado en el procesado de datos diversos y masivos. Sin embargo, el crecimiento y las nuevas formas de captación de datos han llevado a los grandes del sector a adoptar plataformas propias desarrolladas en su mayoría sobre código abierto. El caso de *Apache Hadoop*[284]*, empleada por Facebook, o No SQL*[285]*,* para bases de datos no relacionadas pero masivas, destacan ahora en el tratamiento de informaciones masivas. Por su parte, otras compañías del sector como *SAS*[286] *o IBM,* han sabido ofrecer una combinación de máquina complementada con software para tratamiento masivo de datos.

---

[283] Las máquinas de Oracle y su gestión de grandes bases de datos conformarían todo el inicio del presente siglo al respecto: http://www.oracle.com/technetwork/database/exadata/overview/index.html

[284] Apache Handoop: http://hadoop.apache.org/

[285] Strauch, Christoph. *"No SQL whitepaper*". Recurso disponible en http://www.christof-strauch.de/nosqldbs.pdf

[286] La oferta de paquetes de tratamiento de datos masivos de SAS: http://www.sas.com/en_us/software/data-management.html

Por su parte, el propio desarrollo del hardware (la máquina física sobre la que corren los programas) también *ha* sufrido un cambio de paradigma importante que ha desubicado a fabricantes consolidados. Las compañías cuyo negocio está orientado a Internet, como Google, Amazon o Facebook, han comenzado a apostar por estándares abiertos para la instalación de sus granjas de servidores. El modelo *de Open Compute*[287], ha terminado por obligar a los fabricantes a seguir unos parámetros abiertos y escalables, independiente de cualquier capa administrativa del fabricante. Así, iniciativas como las de Facebook[288] han conseguido forzar las características de un equipo básico y escalable en función a sus necesidades. De este modo no solo se ha conseguido establecer unos parámetros en los que el fabricante de los equipos no puede condicionar la manera en la que se establecen las granjas de servidores de las empresas de Internet sino que estas han conseguido ser las que obliguen a unos estándares abiertos de los que se terminan por beneficiar el conjunto de entidades y negocios que necesiten de grandes servidores.

Mediante los dos procesos descritos, de adecuación de un *software* orientado al gran manejo de información y un *hardware* diseñado expresamente para las necesidades de las grandes empresas, llegamos a un momento en el que la estructuración de estos datos permite a los que los manejan poder operar de forma certera en su negocio. Si entendemos que la mayoría de las compañías de Internet o reside su modelo de negocio en los datos o son al menos una parte esencial de este

---

[287] Open Compute: http://www.opencompute.org/

[288] Sobre Facebook y el modelo Open Compute compuse un artículo recentemente: http://andradesfran.com/facebook-obligando-a-los-fabricantes-a-que-les-hagan-servidores-a-la-carta-mediante-el-open-compute/

la adecuación de su entorno de producción ha posibilitado la expansión que llega a nuestros días[289]. La analítica de datos se ha convertido en la piedra de toque de todo el negocio.

La privacidad frente al Big Data

Nunca en la historia de la humanidad se ha tenido la posibilidad de adquirir tantos datos personales de cada uno de los individuos que componen la sociedad. Buena parte de estos datos son ofrecidos de forma voluntaria, aceptando condiciones de uso (esa parrafada junto al casillero de confirmación que nadie lee) de forma inconsciente. Los medios de vigilancia también han avanzado hasta extremos que podríamos considerar de ciencia ficción. La privacidad y la lucha por mantenerla y tener poder sobre ella se están convirtiendo en uno de los ejes del activismo en la red. Como veremos al tratar los temas de las grandes filtraciones, la exposición a la que nos enfrentamos a diario desde que la red está en todas partes y la mayor parte de la población del mundo más avanzado se conecta prácticamente a diario se ha incrementado. La práctica totalidad de los servicios en línea que se ofrecen hoy en día, adquieren y hacen uso de datos de sus usuarios[290].

En este contexto, ya hemos señalado como la adquisición de la mayor parte de datos posibles de perfiles individuales, desde datos biométricos a pautas de compra, interrelaciones grupales, opinión, poder adquisitivo, consumo de noticias y conexiones a diversos medios en la red puede ser adquiridos mediante nuestra navegación, ya sea desde nuestros

---

289 . Dans, E. *Todo va a cambiar*. Deusto. Madrid. 2010

290 Schönberger, V. Big Data*: A Revolution That Will Transform How We Live, Work, and Think*. Hougton Mifflin Harcourt. Nueva York. 2013

ordenadores personales como desde nuestros dispositivos portátiles, fundamentalmente el *Smartphone*[291].

Todo el rastro diario que los usuarios han ido dejando desde que comenzaran a usar sus cuentas, hace más de una década, en las diversas redes sociales o medios, Facebook, Twitter, YouTube, *EBay*, *Amazon* por ejemplo, así como visitas a blogs o portales con código de rastreo publicitario, como Google A*dWords* u otras *cookies* que persisten, terminan por confluir en un perfil personal que termina por revelar, sin violar ningún termino que hayamos autorizado ni ninguna ley de protección de datos de cualquier territorio, un perfil personal bastante bien delimitado[292].

La red de perfiles y preferencias se alimenta principalmente de nuestra actividad social y nuestra reacción a diversos medios. Según *Techcrunch* [293], un 46% de las entradas a servicios web que piden identificarse se hacen mediante nuestra cuenta de Facebook y en cerca, con un 43%, está Google. La extensión de los marcadores sociales disponibles en la mayor parte de publicaciones, es ya suficiente como para tener un rastreo de preferencias personales bastante fidedigno**.** Así debemos entender la proliferación de *APIs* sociales (aplicaciones insertadas en las webs) que nos ofrecen elevar un comentario en cualquier medio. Para comprender la importancia de estos elementos a la hora de establecer el Big Data comercial mencionaremos cómo Facebook ha sido una de las empresas que más veces ha cambiado los términos de

---

[291] 17. *Sabaté, J. Big data*, ¿una amenaza a nuestra intimidad?: http://www.consumer.es/web/es/tecnologia/internet/2011/12/06/205118.php

[292] . Stéphane Grumbach y Stéphane Frénot. *Los datos, el poder del futuro* (Traducido de Le Monde) http://www.rebelion.org/noticia.php?id=162050

[293] Sobre cómo se alimenta de perfiles sociales nuestras lecturas y reacciones a los medios: http://techcrunch.com/2013/04/08/report-46-of-social-login-users-still-choose-facebook-but-google-is-quickly-gaining-ground/

uso y gestión de niveles de privacidad de sus usuarios, en parte por el constante encuentro frente a legislaciones nacionales sobre la privacidad. Esto ha llegado al extremo de que los servicios de identificación de Facebook funcionen de manera distinta dependiendo de la ubicación del usuario.

Craig y Ludloff[294], nos explican el proceso mediante el que la forma en la que se lleva procesando el Big Data converge en un empleo de los datos personales que cada vez nos expone en mayor grado a ser catalogados de forma precisa mediante empresas privadas. El postulado principal coincide con nuestro planteamiento y distingue entre los que recogen los datos, los que hacen uso de ellos, los que hacen negocio con ellos y los que intentan regular el negocio de los datos personales. Así se prefigura un panorama en el que se avanza de forma contraria al interés de la ciudadanía con elementos de control y perfilado cada vez más precisos.

Diversas organizaciones cívicas, entre las que destaca EFF o EPIC[295] llevan más de una década apuntando a la necesidad de tomar posesión de nuestros datos y ser conscientes de cómo se captan y gestionan. Dado que la mayor parte de estas empresas son entidades de derecho radicadas en territorio estadounidense, la mejor respuesta es la navegación segura. Para ello, se han establecido diversas pautas para dificultar el rastreo y el uso de herramientas que no sean privadas, que no

---

[294] Craig, T y Ludloff, M. *Privacy and Big Data. The Players, Regulators, and Stakeholders*. O'Reilly Media. Massachusetts. 2011. Disponible en: http://shop.oreilly.com/product/0636920020103.do

[295] La Asociación EPIC Electronic Privacy Information Center https://epic.org/ , hace un seguimiento bastante estrecho de las situaciones de vulneración de la privacidad de usuarios de empresas y servicios de Internet.

almacenen los datos que circulan entre usuarios y fundamentalmente que se cifren todos los datos que circulan.

A todas estas cuestiones hay que agregar otros medios de captación de datos personales, entre los que citaremos el uso de tarjetas de crédito, fidelización o de trasporte, el uso de *chips* de radiofrecuencia en cada vez mayor variedad de formas y la videovigilancia. En la obra de Cory Doctorow, *Little Brother*[296], se nos explica todo un itinerario de formas en las que se somos vigilados en una ciudad occidental, en este caso trata de San Francisco, y de cómo la resistencia es ya tomada como conducta subversiva y por tanto *perseguible*. La cuestión de la privacidad adquiere de este modo especial relevancia. Herramientas OSINT (Open Source Inteligence) del tipo *Maltego*[297], *Shodan*[298] o el mismo uso avanzado del buscador de Google mediante *Dorks* [299] (sentencias de búsqueda avanzada) nos permiten conocer hasta qué punto podemos extraer información pública de fuentes accesibles desde Internet, para capturar datos privados y hacer uso de estos[300].

Bruce Shneier[301], nos describe cómo la guerra por los datos personales la libran empresas, gobiernos y *cibercriminales* contra la

---

[296] Doctorow, C *Little Brother*. Disponible en http://craphound.com/littlebrother/download/

[297] *Maltego* es una de las herramientas más populares para recopilar datos a partir de unas pocas pistas iniciales: https://www.paterva.com/web6/

[298] Shodan, conocido como el buscador de los hackers, al permitirnos una búsqueda profunda de elementos no evidentes en ifraestructuras y redes accesibles desde internet: https://www.shodan.io/

[299] Sobre lo que puede revelarnos google mediante el uso de dorks: https://www.exploit-db.com/google-hacking-database/

[300] 26. González Pérez, P. *Ethical Hacking*.0xWorld, Madrid. 2014

[301] Schneier, B. Data and Goliath .*The Hidden Battles to Collect Your Data and Control*

ciudadanía, como cada uno de estos trata de hacerse con la información que le permita manipular a su favor y cómo la única forma de escapar de esta redes es mediante el empleo de herramientas de cifrado y el uso de medios y aplicaciones no propietarias. Así tras la trampa de productos de primer orden ofrecidos gratuitamente, como el gestor de correos *Gmail*, de Google, hay que asumir el costo social de una vigilancia y retención de datos, el riesgo de perder nuestra privacidad. Junto a ello, la total disponibilidad de estos servicios a la voluntad de organismos como la NSA, nos expone doblemente. Schneier es una de las voces más críticas al empleo que se está dando a los datos personales y la obsolescencia de la mayor parte de la legislación, ante las formas de organizarse esa captura de datos en la red.

La mundialización de las bases de datos, mediante perfiles comerciales y estatales expone a la ciudadanía de una forma insospechada a ser fiscalizada durante su práctica diaria de una forma desconocida a lo largo de nuestra historia[302]. Existe un extenso debate acerca de cómo se están gestionando estos datos. Las sucesivas conferencias de las autoridades internacionales de protección de datos[303], cuya última ronda se celebró en Ámsterdam en octubre de 2015[304], hacen hincapié en la necesidad de regular cómo se gestionan y protegen estos datos. La

---

Your World. W. W. Norton & Company. 2015 Ed electrónica en http://www.amazon.com/Data-Goliath-Battles-Capture-Control-ebook/dp/B00L3KQ1LI/

[302] Preuss-Laussionotte, S. *La democracia ante los riesgos de la mundialización de las bases de datos*. En El estado del mundo 2009. Akal, Barcelona 2008.

[303] Conferencia sobre privacidad de las Autoridades internacionales de portación de datos. Resulta muy conveniente revisar las resoluciones disponibles en la web de la convocatoria en México durante 2011. http://www.privacyconference2011.org/

[304] También podemos visitar la documentación de la convocatoria de octubre de 2015, en Ámsterdam así como las coclusiones en: http://www.apc2015.net/

realidad apunta a que tanto la legislación como la aplicación de esta avanzan con retardo respecto a las nuevas pautas que se van imponiendo.

Como en tantas otras ocasiones no es la herramienta la que hay que valorar sino su uso. El manejo masivo de datos se ha convertido en un elemento fundamental de nuestro tiempo, con un crecimiento exponencial a lo largo de la última década. El empleo de su fruto por parte de empresas de Internet y la vigilancia ciudadana, de la que trataremos más adelante, es la cuestión que nos preocupa. La forma en la que todo el asunto se conduce tiene su correspondencia con la ideología predominante y la propia visión que de lo público se mantiene. En este sentido, el conflicto, como hemos visto mantiene varios vectores en lucha. El resultado de ese encuentro es la red que tenemos hoy en día.

3.4 La red en todas partes: Web 2.0 la red semántica y la expansión de los servicios en línea.

A lo largo de la última década del siglo pasado, podemos ubicar el momento en el que las comunicaciones personales y el uso de la informática deja de ser un territorio propio de investigadores o terrenos profesionales muy circunscritos para expandirse y llegar a impregnar todos los elementos de nuestra vida cotidiana. El fenómeno adquiere especial transcendencia en los países más desarrollados. Así de una primera Web de hipertexto, en la que la transmisión de datos apenas pasaba de la comunicación por escrito entre terminales, se ha producido una expansión de capacidades y contenidos que han llevado hacia una convergencia tecnológica en la que diversos medios se han integrado en la red de redes junto con una miríada de aplicaciones que ahora apuntan hacia la red de redes o se integran completamente en esta[305].

El proceso de paulatina imbricación en la red de diferentes procesos ha llegado al extremo de que los diversos terminales apenas tiene una limitada funcionalidad cuando no se encuentran en conexión permanente con esta red mundial. Como proceso paralelo, el auge de la telefonía móvil en la última década del siglo pasado, hasta su absoluta popularización se ha convertido en elemento básico de todo urbanita. La paulatina integración de la red en el entorno doméstico en proceso de conquista del salón y el televisor, transcendiendo el espacio PC doméstico, con ejemplos como las consolas de última generación y los servidores de medios y las posibilidades potenciales que las descargas y el paso de estas a este salón traen consigo, apuntan hacia una sociedad en la que la

[305] Estadísticas sobre aplicaciones de acceso a la web y su empleo: http://www.w3counter.com/globalstats.php

capacidad de conexión permanente y acceso inmediato bajo cualquier medio de electrónica doméstica será una constante.

Esta misma popularización de medios y facilitación en el uso ha llevado a el cuestionamiento por parte de los usuarios, como más abajo veremos, de los medios tradicionales de difusión cultural por medio de libros, discos, o películas, ante la capacidad de su reproducción por medio de dispositivos *multipropósito* , como el Smartphone, tabletas o consolas de videojuegos o de orientación específica, como los lectores de libros electrónicos, con cifras de producción y lectura en aumento[306], a pesar de que parte del consumo no sea superficiado en las cifras que se publican por parte de las editoriales[307]. Como veremos en capítulos posteriores, la inadaptación a las nuevas formas de difusión de medios, de distribución y acceso, han propiciado la expansión de formas alternativas de distribución de productos culturales, a las que se cataloga de "piratería" sin ofrecer alternativas realmente viables que no sean las formas precedentes de un mercado abocado a la irrelevancia.

La red en todas partes. La universalización del acceso a Internet.

La web, como se había establecido en el periodo de entresiglos y sobre todo tras la explosión de la burbuja de las *puntocom*, entra en un nuevo periodo de expansión y madurez al calor de la expansión de las comunicaciones, con la posibilidad de acceso casi ubicuo, mediante redes

306 INE. Informe sobre el impacto de la lectura digital en España: http://www.ine.es/ss/Satellite?L=es_ES&c=INECifrasINE_C&cid=1259932520217&p=1254735116567&pagename=ProductosYServicios%2FPYSLayout

307 Informe *Global eBook 2015*. Un documento de Rüdiger Wischenbart, en el que se detalla el estado internacional del mercado del libro electrónico: http://www.global-ebook.com/

inalámbricas primero y más adelante con el uso de telefonía de datos con incrementos en anchos de banda que llegan, en la fecha en la que redactamos a igualar las de la red convencional. Esto quiere decir que cualquier usuario de servicios de la red puede hacer uso de los servicios más comunes sin notar diferencias ni importar la ubicación en la que se encuentre. La web ha llegado a todas partes[308].

Las mismas posibilidades del ordenador clásico, una vez popularizado en cuanto a precios y a una interfaz cada vez más sencilla e intuitiva de emplear, han dado un salto exponencial con la denominada Web 2.0, con aplicaciones como las de Voz-IP (llamadas encaminadas de forma digital), las redes sociales, el vídeo digital, incluso con la difusión de medios y películas a través de Internet, por medio de *podcast* y *streaming*, las *Mashup* (aplicaciones híbridas entre lo instalado en el PC y en el acceso a red), los blogs (páginas personales o colaborativas), videoblogs o las formas participativas de las *wikis*, con la Wikipedia como su forma más reconocida de construcción de agregado cooperativo. Heredero de este, el Smartphone, la *Phablet* (teléfono con una gran pantalla superior a las 5'5 pulgadas) y la Tablet, se convierten en el medio primordial de acceso a Internet y de consumo de datos. Su popularización se asienta a finales de la primera década del presente siglo y el abaratamiento de terminales y tarifas a lo largo de la segunda década hacen que estos dispositivos sean el medio más utilizado[309].

Esta expansión ha ido acompañada de la penetración de un mercado de las telecomunicaciones que no siempre ha avanzado al ritmo

---

[308] Manuel Castells. *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad.* Plaza & Janes. Barcelona. 2001

[309] Estudio de *Nielsen* sobre el uso del Smartphone: http://www.nielsen.com/us/en/insights/news/2015/so-many-apps-so-much-more-time-for-entertainment.html

adecuado entre legislaciones y operadores. El caso del 4G en España, la tecnología de conexión más avanzada que mantenía una de sus mejores frecuencias, la banda de los 800 MHz, ocupada por un grupo de canales de la Televisión Digital Terrestre hasta diciembre de 2014, ha supuesto un capítulo curioso de mal diseño a la hora de prever la extensión de las comunicaciones y que mantuvo un proceso judicial enfrentando a operadores de televisión con compañías de telecomunicaciones que aspiraban a usar la misma frecuencia. El llamado Dividendo Digital[310], el reparto de las diversas frecuencias, dejó a España fuera de las directrices ya sugeridas por la UIT, organización internacional de telecomunicaciones, al cederles a las televisiones digitales parte de un espectro que ya se sabía que debía reservarse para la cuarta generación de datos de banda ancha móvil. A pesar de esto, España se sitúa ya en cabeza europea de la penetración digital con un 82% en el uso de Smartphone, según encuesta del INE de 2014[311].

La importancia de los dispositivos móviles deriva también de la capacidad de extensión de servicios entre grupos de población que no contaban con otros medios de acceso. La adecuación de los servicios, aplicaciones y la misma web, en la que cada vez se implanta más el uso de diseños denominados *responsivos* (adaptables a diversos tamaños de pantalla). Compañías como Google han tenido muy en cuenta el uso de aplicaciones móviles y anunciaron que a partir del 17 de abril de 2015, penalizarán en su buscador las páginas que no tengan diseños adaptables

---

310 Sobre el Dividendo Digital: http://www.televisiondigital.gob.es/DividendoDigital/Paginas/que-es-dividendo-digital.aspx

311 INE*: Encuesta sobre equipamientos y uso de tecnología en España*. Octubre de 2014: *www.ine.es/prensa/np864.pdf2*

para uso por móviles[312]. Así vemos como también la propia red se ha ido adaptando de forma paulatina al uso portátil de sus medios y la extensión entre una población cada vez con menores nociones informáticas[313]. La facilidad de uso, es de este modo el último pilar sobre el que se asienta la presente expansión de la red. En ello, sistemas operativos móviles como iOs, de Apple y Android, auspiciado por Google han jugado un papel fundamental en la última oleada expansiva de la red[314].

Al respecto, diferentes empresas, comenzando por las dos mencionadas, se disputan el tiempo de uso de cada usuario para que permanezcan en sus respectivas aplicaciones. Mayor tiempo de permanencia se corresponde con una mejoría en las perspectivas de negocio y por tanto, no debe extrañarnos como cada una de las opciones trata de establecer un ecosistema propio de aplicaciones con las que ofrecer al usuario toda la experiencia de consumo de medios que pueda necesitar. El hecho de que casi el 84% de uso de terminales móviles en EEUU se concentren en cinco aplicaciones demuestra la importancia del tema [315]. Estos datos, de 2015, nos revelan también la creciente

---

[312] Google, principal beneficiario del auge de la tegnología móvil, detalla en su web de desarrolladores sobre el diseño optimizado para móviles: https://developers.google.com/webmasters/mobile-sites/?hl=es-ES&utm_source=MFT&utm_medium=incoming-link&utm_campaign=MFT

[313] Eurostats nos ofrece una cifras de uso de Internet móvil : http://ec.europa.eu/eurostat/help/new-eurostat-website?p_auth=jVcHEUXV&p_p_id=estatsearchportlet_WAR_estatsearchportlet&p_p_lifecycle=1&p_p_state=maximized&p_p_mode=view&_estatsearchportlet_WAR_estatsearchportlet_action=search&text=Individuals+using+a+mobile+phone+via+UMTS+%283G%29+to+access+the+internet

[314] Tendencias internacionales 2015 del mercado de las comunicaciones móviles: http://www.budde.com.au/Research/Global-Mobile-Communications-Market-Insights-Statistics-and-Regional-Trends.html

[315] Artículo de Techcrunch a propósito de los usos y tiempos de empleo del Smartphone: http://techcrunch.com/2015/06/22/consumers-spend-85-of-time-on-smartphones-in-apps-but-only-5-apps-see-heavy-use/#.p436dj:WjjV

concentración de medios. Por ejemplo, Facebook, que junto a la red social aglutina *Instagram* y *WhatsApp* acumula el 13% de los tiempos de uso. Google, que junto a YouTube como servicio estrella, cuenta con Gmail, Maps o Google Now, acumula el 12% de esos tiempos. El resto lo ocupan conocidos de la red como Apple, Yahoo! eBay o Microsoft. Más allá del dato, la tendencia a acumular la multiplicidad de usos de la red, han llevado a una carrera por copar nichos de mercado y a unas políticas de adquisiciones y competencia desmedida. El capítulo más reciente es el de la música en *streaming* (difundida desde la propia red). Spotify, surgiría en 2008 como un servicio pionero y una auténtica alternativa a las descargas ilegales de música. Por una tarifa de 9,9€, para las suscripciones *Premium (con todas las mejoras)* ofrecía acceso a una gran biblioteca musical, a la que se puede acceder con una conexión de datos superior a los 256 kbit/s mediante un protocolo *P2P* [316] . Algunas alternativas independientes *como Deezer, SoundClud, Grooverhark o Rdio* compitieron en diversos segmentos con esta aunque el éxito de *Spotify* ha sido arrollador a lo largo de esta década. Ante este panorama tanto Google, con *Google Play Music*, como Apple más recientemente, con *Apple Music*, han entrado a competir igualando el catálogo de esta, que ronda los 30 millones de canciones. La cuestión no es tanto, el mercado como los usuarios que están ahora mismo fuera de su ecosistema, que trata cada vez de estar más *integrado,* sistemas de pago propio incluido. Desde luego este es tan solo un ejemplo pero ilustra de forma bastante detallada un escenario que se hacer recurrente en la actualidad, el de la búsqueda de ocupar todos los nichos de mercado por parte de los grandes de Internet.

316 Spotify,será el servicio pionero en *streaming* musical: https://www.spotify.com/es/

Web 2.0. Nuevos usos e interacción con la red y explosión de las comunicaciones.

El término Web 2.0 [317] será acuñado en 2004 por Dale Dougherty de la compañía *O'Reilly Media*, en una conferencia en la que compartió una lluvia de ideas junto a Craig Cline de *MediaLive*. En ella, distinguirían esta nueva forma de acceso a la red múltiple, abierta y más participativa, a la luz de la expansión de las *puntocom*, en la que la Web es entendida como una plataforma de medios en la que la información que se mueve a través respecto al modelo precedente estático y no reactivo. Así, vemos como la clave estará en la manera en la que la información es proporcionada y la forma en la que actúa respecto al usuario. A diferencia de la forma anterior estática y servida de forma en la que el usuario dispone de ella de forma pasiva, ahora es suministrada de forma participativa y multidireccional. Aunque a veces se establece similitud entre esta Web 2.0 y la Web semántica, esta última sería el resultado de la primera; una suerte de evolución hacia una forma aún más interactiva entre contenidos y peticiones, de disponibilidad inmediata[318].

En la siguiente fase de expansión de la red, se pierde en carácter profesional de esta para expandir los servicios y el ocio hasta convertirse en la clave principal que moviliza la mayor parte del tráfico de red que se genera actualmente, con una proliferación de servicios capaces de acaparar a millones de usuarios activos, como han logrado redes sociales como *Facebook*, la inserción de fotos de viajes mediante *panoramio*[319] en

---

[317] Cobo, C. y Pardo H. *Planeta Web 2.0. Inteligencia colectiva o medios fast food.* Grup de Recerca d'Interaccions Digitals, Universitat de Vic. Flacso México. Barcelona / México DF. ,2007 (con licencia CC disponible en http://www.planetaweb2.net/)

[318] García, C. y Arroyo D. *Biblioteca Digital y Web Semántica*. Disponible en: http://biblioweb.sindominio.net/telematica/bibdigwebsem.html

[319] 15. http://www.panoramio.com/

Google Maps o colecciones de fotos personales y profesionales en Flickr[320], con casos como el de una suerte de galería de arte en red de Devianart(17). En lo que respecta a los aspectos sociales, la red se convierte en la base de una ebullición de productos y redes en las que la interacción entre usuarios será la clave. En poco tiempo, se avanzará a una interconexión más estrecha a través de la red, hasta desplazar los usos convencionales del teléfono. Nuevas formas de comunicación instantánea superaran esa herencia con los foros que seguían manteniendo las redes sociales al uso. Así, la presente década asiste al ascenso de nuevos medios de comunicación tanto grupales como individuales, instantáneos entre los que destacan *WhatsApp, Telegram o Line,* dependiendo de la zona geográfica en la que predominan.

Otros casos también reseñables como Second *Life*[321], se han correspondido más a esa burbuja de las *puntocom*, en la que el concepto ha superado a la realidad objetiva. Así, lo que se suponía la enseña del *metaverso*[322], un mundo virtual en el que las personas, mediante *avatares* (personalidades virtuales) se interrelacionaban en un mundo abierto a todas las posibilidades quedaría pronto en desuso. Con una sagaz campaña comercial, por parte de la empresa Linden *Research Inc.* en 2003, este universo virtual fue capaz de atraer, desde su

[320] Flikr sería durante años el servicio de referencia en lo que respecta a fotografía digital. Dependiente de Yahoo!, ahora mismo comprte el declive general de la compañía matriz: 16. http://www.flickr.com/

[321] Second Life es para muchos un caso paradigmático de plataforma sobrevalorada: http://secondlife.com/

[322] El termino *metaverso* y el de un universo virtual seria sugerido por primera vez en la novela de Neal *Stephenson, Snow crash.*

lanzamiento, todas las miradas que, en parte gracias a la nueva mitología de la ciencia ficción, como *Matrix, de los* Wachowski, en el cine, o la novela *Neuromante* de Gibson, entre otros habían "preparado" a la audiencia. Como señalamos, comercialmente se ha tratado de uno de los mayores éxitos de su momento, al conseguir que todo tipo de empresas y organismo, incluso el instituto Cervantes [323] quisieran ubicar tiendas virtuales dentro de este mundo. Efectivamente, *Second Life* será uno de los mayores *hypes* (neologismo que hace referencia a una expectativa hiperbólica) del siglo. Se llegó a un momento en que incluso se abrieron iglesias y políticos dieron mítines dentro del universo virtual. Una de las ideas más rentables para la compañía en cuestión sería la de establecer una moneda virtual dentro de *Second Life*, los *Linden Dollars*, con los que se podían comprar múltiples servicios y accesorios para nuestros avatares. La conversión de estos a moneda real sería un proceso bien rápido y pronto aparecería en todas las noticias Anshe Chung [324], como la primera millonaria gracias al trabajo dentro de un mundo virtual. A pesar de ello, la impresión que un usuario puede sacar de Second Life, después del boom primero de este mundo, y de los 13 millones de usuarios registrados que declarase en su momento, era la de un mundo vacío, en el que el potencial que los medios han señalado supera la realidad de un mundo virtual *inmersivo* con poco que hacer cuando no hay grupos formados al estilo de otra red social y que terminaría desinflándose ante el abandono de sus usuarios.

---

323 http://secondlife.cervantes.es/es/default.htm

324 http://www.anshechung.com/

Dentro de estos mundos de inmersión *online*, serán los juegos multijugador los que atraigan mayores audiencias. Como vimos, incluso el Departamento de Defensa estadounidense, mantiene su juego, imitando el éxito del juego en primera persona *Counter Strique,* America's Army[325], como medio de captar jóvenes para el ejército en un lugar más atractivo para estos y que contaría con servidores propios y de descarga gratuita. De cualquier modo, el gran juego de rol multijugador masivo (MMORPG) que, a pesar de ser de pago, ha llegado a más de 11 millones de usuarios activos es *World of Warcraft (conocido como WOW entre los usuarios)*[326], aparecido en 2004, al calor del aumento en la calidad de conexión, por parte de la compañía *Blizzard*. WOW se encuentra inserto dentro de un mundo de fantasía heroica, en el que dos grandes facciones de jugadores se disputan zonas de ese mundo, comercian y desarrollan posesiones. Esto ha hecho que este juego sea uno de los más observados por estudios de economía y de psicología, tanto en el estudio de precios de mercado como en el aspecto social, sobre todos cuando se han dado casos como el de *la plaga*, en septiembre de 2005, un fallo en el juego que infestaba literalmente a los personajes del juego hasta llevarlos a la muerte. Este caso, ha servido como forma de estudiar pautas sociales ante epidemias, al observar como muchos de estos jugadores, conscientes de la enfermedad de su personaje, acudían a las grandes ciudades contagiando a otros[327]. El caso de la economía virtual es otro de los grandes procesos de estudio de este juego, en el que se ha dado un proceso de venta de oro

---

[325] Americas Army. El videojuego diseñado para reclutar soldados en EEUU: http://www.americasarmy.com/

[326] World Of Warcraft será un juego masivo Multijugador online capaz de crear sus propios memes y una economía capaz de trascender al juego: 23. http://www.wow-europe.com/es

[327] Noticias sobre la plaga en el WOW: http://news.bbc.co.uk/2/hi/health/6951918.stm

(la moneda del juego) o de otros elementos del juego de forma no del todo ajustada a las normas del este, en teoría no permitido. Esto ha dado pie a un fenómeno masivo de *Gold Farmers* (granjeros de oro), sobre todo en China, que se dedican de forma profesional a ofrecer servicios a los jugadores, previo pago real. En algunas de las grandes ciudades, la presencia de estos vendedores, que acosan a jugadores o hacen campañas publicitarias chocantes, a pesar de que *Blizzard* bloquea supuestamente a los que realicen estas prácticas nos avanza lo que puede esperarnos en un futuro en el que estos mundos comiencen a extenderse entre la población. La forma de interactuar con el juego, hecho social, con medios propios como Steam[328] ha cambiado la perspectiva del futuro online. Novelas como Ready Player One[329] apuntan a un futuro en el que lo lúdico y lo académico convivirán de forma indisociable.

El caso de Google merece una mención singular, al tratarse de la gran enseña de esta nueva Web, desde que su buscador se convirtiera en la gran fuente de búsquedas, gracias a su motor mucho más sofisticado que sus competidores, y a la integración paulatina de nuevas formas de entender procesos hasta entonces fijados a lo local y vinculados a una máquina. De este modo, herramientas como *Pagerank* (que establece categorías de diversas páginas para aparecer en sus búsquedas) o *Adsense* (que ofrece la posibilidad de insertar publicidad gestionada por Google en cualquier página como comisionista) son la base de su negocio digital. Asimismo, la novedosa forma de tratar el correo con *Gmail*, tratar documentos con Google Docs o incluso ver mapas y fotografías de satélite con búsquedas por ubicación integradas, en *Google Maps* o su versión

---

328 Steam es la mayor plataforma de juegos multijugador: http://store.steampowered.com/

329 26.Cline, E. *Ready Player one*. Ediciones B. Barcelona. 2011.

instalable *Google Earth*, ha marcado las pautas de otros servicios de la Web 2.0. Esta compañía, ajustada, como tantas otras grandes del sector, al mito fundacional de jóvenes que apuestan por una creación concreta partiendo desde cero, a pesar de unas prácticas que de ser llevadas por otros ya habrían estado en el ojo del huracán sobre monopolios[330], ha sabido ganarse la simpatía de todo el sector más implicado en las nuevas tecnologías, precisamente con una política visualmente contrapuesta a las de otras compañías, especialmente *Microsoft*. De este modo, la posibilidad de incorporar desarrollos libres, códigos abiertos y unas prácticas empresariales más "amigables" respecto a los usuarios, no vistos como sospechosos permanentes de "piratería", hicieron que esta compañía pudiera llevar prácticas empresariales que, en otros casos habría sido puesto en cuestión[331]. Los últimos tiempos, en los que la posición de domino y unas políticas más restrictivas junto con la supresión de servicios muy reconocidos entre la comunidad como Google Reader (su lector de noticias vía RSS) hicieron que se cuestionara la máxima fundacional de la marca "*Don't be evil"* (no seas malo). En la actualidad la compañía se enfrenta a una fiscalización por parte de la UE en los aspectos del derecho al olvido (derecho a borrado de datos pasados por parte del usuario), su agregador de noticias e incluso en la forma en la que se ofrecen los resultados de sus búsquedas.

Por último una de las industrias que mayores beneficios encuentran en la red y que mejor se han adaptado a esta es la de la pornografía. Desde la primera fase de expansión, la pornografía ha sido tanto una de mayores fuentes de tráfico de red como de contenidos descargados de forma no

---

[330] 27.Suárez Sánchez Ocaña, A. *Desnudando a Google*. Deusto. Madrid. 2012

[331] 28. Reischl, G. *El engaño de Google*. Medialive Content. Barcelona. 2008

legal. Los datos de 2010[332] revelan que cómo agrupa un 25% de las búsquedas, el 12% de los sitios de Internet son pornográficos o que el 35% de las descargas sean de este tipo de contenidos. Sitios como *Pornhub*[333], uno de los portales de vídeo con mayor implantación en la red, pública sus estadísticas anuales y apunta cómo la tecnología móvil también se apunta con fuerza al consumo de sus contenidos [334] . Así a lo largo de sus estadísticas nos revelan el incremento en España del consumo de vídeo con dispositivos móviles alcanza en conjunto el 51% de las peticiones totales[335]. Tanto los servicios de suscripción y descarga de pago, como los portales con publicidad y las descargas ilegales hacen de la pornografía una de las industrias más vitales de la red y una de las más resistentes a la censura. Los experimentos con realidad virtual e incluso los juegos, apuntan a que la industria seguirá siendo puntera se integre o no con los grandes de la industria de Internet.

La Brecha Digital.

Como contrapunto a todo este periodo de expansión, la parte excluida o incapaz de acceder a los nuevos medios nos muestra un incremento de la desigualdad. La red ha comenzado a expandirse a lo largo de todos los usos sociales y forma parte del consumo diaria de cada vez más población. La denominada Brecha digital se abre entre los que

---

[332] Infografía de la web Gizmodo con algunos datos relevantes sobre la pornografía en Internet: http://gizmodo.com/5552899/finally-some-actual-stats-on-internet-porn

[333] Las cifras del porno. Estadísticas anuales (2014) del portal PornHub, uno de los mayores del mundo, sobre usos y accesos a sus contenidos: http://www.pornhub.com/insights/2014-year-in-review

[334] Cifras de 2013 http://www.pornhub.com/insights/pornhub-2013-year-in-review/

[335] El ranking de Alexa de las páginas de temática adulta más visitadas en España: http://www.alexa.com/topsites/category/Top/World/Espa%C3%B1ol/Adult

tiene acceso o no lo tienen. A esto hay que añadir otro facto entre los países más desarrollados y es la denominada Brecha Generacional, en lo que respecta al acceso a Internet[336]. Así se establece una clara línea entre los que tiene acceso a los nuevos medios y los excluidos. Una nueva forma de exclusión y pobreza se perfila en torno a esta capacidad de acceso y manejo de los nuevos medios de los que disfruta el mundo desarrollado y dentro de este los que tiene capacidad de acceso tanto formativa como socioeconómica.

En el año 2000 menos de un 20% de la población española había accedido Internet en alguna ocasión. Las cifras de 2014 apuntan ya al 76,2% de la población adulta. Buena parte de este acceso de los últimos tiempos se debe al despliegue de la tecnología móvil y la ampliación del acceso. Esto no resta calidad al dato pero lo matiza para realizar un análisis certero. No solo se trata del acceso a la red sino de la capacidad de establecer una comunicación oficial, manejar un certificado digital o redactar un correo electrónico. Así la falta de una definición concreta del término nos puede llevar a cifras engañosas acerca de la exclusión exacta que supone la divisoria definida en el término brecha digital[337].

La pobreza informacional, todavía a medio camino de ser definida, a pesar de los intentos de La Estrategia Europa 2020 o las recomendaciones metodológicas Eurostat (Oficina de Estadística de la Unión Europea) quedaría definida no solo por la incapacidad de acceder y comprender el uso de Internet, sino por la posibilidad de tener siquiera acceso y poder hacer un uso adecuado de este[338]. A entender del que escribe, queda

---

[336] Serrano, A y Martínez; E. *La Brecha Digital: Mitos y Realidades*, Editorial UABC, México, 2003, Disponible en: www.labrechadigital.org

[337] Fundación Alternativas: Informe de 2014 sobre la brecha digital en España: http://www.fundacionalternativas.org/actividades/presentaciones/la-desigualdad-digital-una-nueva-fuente-de-desigualdad-politica

[338] INE datos sobre la brecha digital http://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528782&p

mucho camino por definir al respecto, dado que los datos que se nos brindan tan solo separan géneros y edades sin especificar más parámetros.

=1254735110672&pagename=ProductosYServicios%2FPYSLayout&param3=1259924822888

3.5 El sistema de patentes como instrumento. Trolls de las patentes y guerra en la innovación.

El sistema de patentes está ligado al propio desarrollo de nuestra era y su sistema económico. Desde que se iniciase la sociedad industrial, este mecanismo ha servido como supuesta forma de garantía para la inversión en innovación. Así, quien patenta alguna invención, adquiere un derecho reconocido por la oficina de patentes correspondiente, que le otorga la exclusiva potestad sobre lo registrado. Los derechos registrados de esta forma permiten al titular comerciar con estos para ceder su uso a terceros, cobrar una licencia, vencerlos, heredarlos y en general disponer de estos de forma similar a cualquier otra propiedad. En un entorno aséptico, en el que la investigación es reconocida con estos derechos que garantizan el retorno de la inversión protegiendo la exclusiva de explotación durante un tiempo determinado, la idea de rentabilizar el esfuerzo, a modo de recompensa por la innovación será aceptable. La realidad es que el uso mercantil de las patentes ha degradado hasta prácticas y usos que en nada encajan con esta descripción primera. La economía informacional, en palabras de Castells[339], es eminentemente capitalista y como tal, busca el beneficio y la "eliminación sistemática de competidores" mediante cualquier instrumento.

Como veremos, en lo que respecta a nuestra investigación, el sistema de patentes ha jugado un papel estratégico en cuanto a la lucha competitiva entre empresas y estados. Se ha jugado con elementos de difícil interpretación para disputar con rivales económicos aspectos

[339] VV.AA. Sociedad Mediatizada. Gedisa. Barcelona.2007

comerciales, retasar lanzamientos de productos, laminar mercados o impedir el desarrollo de una competencia efectiva. Todas estas estrategias se han trenzado en un doble frente legal y político. Por un lado, contando con el papel de ciertas oficinas nacionales de patentes que se han prestado a registros absurdos o inútiles por otro, con unas prácticas de *lobismo* que han llegado a debates en instancias internacionales fuera de cualquier interés ciudadano.

Las líneas rojas de lo "patentable" se convirtieron en aspectos difusos con el ascenso de las nuevas tecnologías y la sociedad de la información. Los conceptos que anteriormente se encontraban claramente definidos, se desdibujan bajo el patrón de entornos en los que buena parte de los recursos se definen mediante software, muchas veces de forma independientemente del medio de acceso. El copyright y las patentes se han convertido en uno de los instrumentos políticos de mayor calado y una de las zonas de mayor influencia en la sociedad de la información[340]. Su demarcación no solo afecta a aspectos concretos sino que la onda de su alcance puede definir completamente el marco de desarrollo económico ligado a las empresas, a internet y a la evolución de soluciones "paralegales" o alternativas no reconocidas legalmente por los estados y que precisamente muchas de estas iniciativas sin alternativas viables no han hecho más que potenciar. Si estamos definiendo el ascenso de la sociedad de la información y el Internet que tenemos hoy en día como un proceso de conflicto de intereses y una constante dialéctica entre elementos contrapuestos de mercados, gobiernos y ciudadanos, el territorio de las patentes es uno de los escenarios en los que esta lucha se

[340] Stallman y otros. Contra el Copyright. Tumbona Ediciones. México. 2008. Edición electrónica: http://bibliotecalibre.org/handle/001/352

escenifica más claramente. Como veremos, sucesivos intentos de restringir la competencia, los desarrollos libre o el lucro menos ético han concurrido en torno al tema de las patentes en un breve periodo de tiempo[341].

Las patentes de software

Uno de los primeros frentes de este conflicto ha sido la posibilidad de patentar el software. La centralidad de este en la nueva economía juega un papel esencial en la estrategia comercial de naciones y empresas. Su regulación jurídica ha experimentado una rápida evolución, más que por su novedad por el empuje de las grandes compañías que comercian con el[342]. Efectivamente, se trata del sector más representativo de esta "nueva economía" y por tanto su papel idealizado de paradigma de prosperidad del sistema. El software, mas como conocimiento que como bien comerciable, difícilmente tiene un encaje jurídico en el sistema de patentes tal y como ha sido definido hasta nuestros días.

El profundo debate acerca de la patentabilidad del software enfrentaría a una industria bien organizada en lobbies, (fundamentalmente norteamericanas) frente a activistas del software libre, colectivos ciudadanos y pequeñas y medianas empresas europeas. Estos últimos manifestaron su posición contraria a que se pudieran patentar aspectos

---

[341] Lessig.L. *Por una Cultura libre. Cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad*. LOM. Santiago, 2005. Edición electronica: http://www.traficantes.net/libros/por-una-cultura-libre

[342] Stallman, R. *Software Libre para una sociedad libre*. Traficantes de sueños Ed. Madrid. 2013. Edición electronica: http://www.traficantes.net/libros/software-libre-para-una-sociedad-libre

esenciales para el funcionamiento común de la mayor parte de las rutinas informáticas. En este sentido, poseer patentes que restringieran usos comunes significaría apoderarse de sectores completos del mundo informático y cerrar el acceso a todo software libre que como tal no actúa no ánimo de lucro. El acceso al software condiciona la capacidad de cualquier desarrollo. El control tecnológico privado del software es equivalente a la apropiación privada del alfabeto en los orígenes de la historia[343].

Cualquier software medianamente desarrollado cuenta con miles de líneas de código, que se sustentan en desarrollos anteriores o implementan técnicas ya desarrolladas. La innovación completa desde cero no existe como tal. Ninguno de los desarrollos actuales, aun empleado lenguajes de programación novedosos, incluso reinventados, parte de unos conceptos previos de un bagaje intelectual del que no puede abstraerse. De este modo, no resultaría difícil poder encontrar fragmentos de código concurrente en prácticamente cualquier programa que nos permita examinar su código[344].

La "travesía legal" de la patentabilidad del software no era algo nuevo en los EEUU. Ya en los '80, WIPO (World Intellecutal Property Organization) terminaría excluyendo los programas y su código fuente de la patentabilidad. En aquellos momentos software y hardware estaban todavía ligados en sus aspectos comerciales. Sin embargo, ya en 1976, La *Copyright Act*, fijaba en EEUU la primera protección para el software,

---

[343] VVAA. *Cultura digital y movimientos sociales*. Catarata. Madrid. 2008

[344] Lessig.L. *El código 2.0.* Traficantes de sueños (licencia Creative Commons), Madrid. 2009.

equiparándola al Copyright, aunque quedaban excluidos de esto los "algoritmos matemáticos. Una indeterminación que se concretaría más en 1994, al definir como patentable todo lo que sea distribuido en soporte físico, disco o Cds en su momento. La Oficina de patentes estadounidense fijaría ese mismo año las normas de patentabilidad, abriendo la primera puerta a la patentabilidad de programas y multiplicando sus registros. La nueva agenda digital elaborado por WIPO, establecería las pautas para extender esta visión globalmente. Sin embargo, Europa, distinguía entre programas concretos y algoritmos. Si bien El Convenio Europeo sobre patentes prohibía las patentes de software, la Oficina de Patentes Europea (EPO), se financiaba de manera autónoma con las licencias que inscribía y no aplicaba este convenio. Los conflictos respecto a patentes tampoco son nuevos en Europa pero no sería hasta 2005 cuando se planteara la primera directiva europea sobre patentes de software. Una turbulenta negociación donde diversos actores externos entrarían en juego llevaría un debate que escapó del ámbito del parlamento y la comisión de la mano de movimientos ciudadanos[345].

El conflicto por la patentes llegaría a debate en la UE de la mano de la Business Software Alliance (BSA)[346] , grupo de presión para las grandes compañías estadounidenses sin inversiones en Europa que en 2003 lograría introducir el debate en su seno. El 7 de marzo de 2005, el Consejo Europeo, compuesto por los ministros de Industria y Energía de los 25 estados europeos, aprueba la "*Directiva sobre la patentabilidad de las invenciones implementadas en ordenador",* es decir, las patentes de

[345] La Free Software Foundationelaboraría un interesdnte documento sobre el initnerario de las patentes de Software en Europa: https://fsfe.org/campaigns/swpat/background.es.html

[346] La BSA y sus miembros: http://ww2.bsa.org/country.aspx?sc_lang=es-ES sus Integrantes se encuentran detallados en: http://ww2.bsa.org/country/BSA%20and%20Members/Our%20Members.aspx

software[347]. La reacción ante tal directiva movilizaría a buena parte del activismo europeo, organizaciones de libertades ciudadanas y defensoras del software libre así como buena parte de la izquierda europea que desde la oposición asistió a la aprobación de una directiva sin un debate abierto. Así el 6 de julio de 2005 una mayoría de 648 de los 680 votos posibles, el Parlamento Europeo rechazó por completo la directiva de patentes de software. En el camino quedaría una negociación truculenta, en la que resulta complicado delimitar entre practicas lobistas y corrupción (la ya famosa puerta giratoria) y en el que ningún grupo, incluso dejando expuestos a sus propios ministros, quiso ser retratado en esa directiva[348] .

La comunidad que defiende el Código Abierto (Open Source), sería la gran triunfadora de este choque, al conseguir que el Software libre no fuese acorralado por una legislación diseñada por las compañías de la BSA. La ética de la comunidad del software libre pudo imponerse gracias a un activismo europeo vigilante de las negociaciones que de forma más o menos encubierta se celebra en el seno de la UE. El establecimiento de redes de organización establecerá, junto con el rechazo al acuerdo del ACTA, un camino de vigilancia constante que encontrara en la red su forma natural de respuesta como veremos en capítulos sucesivos[349].

El mismo escenario se repetirá casi una década después con respecto a la neutralidad de la red. Los debates se suceden a lo largo de 2015 y aunque algunos de los actores son diferentes, las maneras son muy

---

[347] VVAA. *Cultura digital y movimientos sociales*. Catarata. Madrid. 2008

[348] FSF. *Cronología de la Ley de patentes en Europa*: https://fsfe.org/campaigns/swpat/status.es.html

[349] Ugarte de, D. *El poder de las redes*. Colección Biblioteca de las Indias. Madrid. 2011

similares[350]. Asimismo, se vuelve a sugerir la patentabilidad del software, esta vez por parte del gobierno de España, con un borrador de reforma de la legislación española de patentes que será debatido a lo largo de 2015[351] y que contiene en su texto menciones expresas[352]. Que la cuestión sea planteada de forma tan recurrente apunta a un diseño externo que se niega al cierre del debate y lo vuelve a plantear en todas las instancias receptivas a su capacidad de *sugestión*[353].

Como vemos, la tensión entre los que defienden un software libre[354] , a disposición de quien quiera usarlo y la de la contraparte que busca un control absoluto sobre la producción informática, tratando de imposibilitar desarrollos independientes ha vivido momentos de extrema tensión[355]. Sin embargo no todo el contexto se divide entre dos extremos. Empresas como Google, potenciaron el desarrollo de Software libre tanto en telefonía, con la plataforma Android, en contraposición con el cierre de Nokia con *Symbian*, que lo llevaría a la debacle comercial, como incluso en el terreno

---

350 Campaña de la FSF por el fin de las patentes de Software (2015): http://endsoftpatents.org/

351 Informe de la asociación española Xnet: *Las partes más sospechosas de la nueva ley de patentes española*: https://xnet-x.net/ley-patentes-como-tal/

352 Congreso De España Borrador de reforma de la Ley Española de Patentes. 24 de Noviembre de 2014:https://intranet.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-10-A-122-1.CODI.%29#%28P%C3%A1gina1%29

353 Oficina Española de patentes y Marcas: Folleto informativo donde se defiende el supuesto beneficio de las patentes de software y explica su procedimiento: http://www.oepm.es/cs/OEPMSite/contenidos/Folletos/FOLLETO_3_PATENTAR_SOFTWARE/017-12_EPO_software_web.html

354 Castells, M. *Internet, libertad y sociedad: una perspectiva analítica*. Lección inaugural del curso académico 2001-2002 de la UOC. http://www.uoc.edu/web/esp/launiversidad/inaugural01/intro_conc.html#

355 La definición de software libre y el uso de CopyLeft: http://www.gnu.org/philosophy/free-sw.es.html

de los navegadores, con *Chromioun* como enseña (el desarrollo libre de Chrome que prueba las mejoras antes se der implantadas). Así, llegaría al extremo de permitir el uso de sus patentes a todos aquellos desarrolladores que destinaran su trabajo a plataformas libres[356]. Por otra parte, junto a Facebook, han sabido confrontar con las empresas de tecnología al definir el modelo Open Compute, como hemos visto en capítulos anteriores.

La guerra de patentes en Android

Apple, a instancias de su entonces CEO Steve Jobs, iniciaría una campaña de demandas contra buena parte del ecosistema Android con sucesivas denuncias por vulneración de patentes contra HTC, Samsung y Google[357]. El alcance de dicha campaña mantendría durante varios años en una situación precaria a fabricantes como Samsung o HTC, provocando retrasos en los lanzamientos de muchos de sus productos y unos costes legales ingentes que terminarían en una cadena de acuerdos y una rebaja de tensiones a lo largo de 2014.

En abril de 2011 Apple demandó a la empresa surcoreana Samsung por plagiar el diseño de sus teléfonos iPhone y tabletas iPad. Samsung respondió con una contrademanda, en la que acusaba de otro tanto. Curiosamente, en el momento de la demanda, Samsung fabricaba para Apple el 80% de los componentes de sus terminales. Precisamente al calor de la permisividad de la oficina de patentes de EEUU a la hora de

---

[356] Sobre el permiso de Google a emplear ciertas patentes de su propiedad si son empleadas en proyectos de Código Abierto: https://www.eff.org/deeplinks/2013/03/google-makes-open-patent-non-assertion-pledge

[357] Isaacson, W. *Steve Jobs*. Trinith & Banshee. Nueva York. 2011

registrar ideas, la multiplicidad de patentes que enfrentaban a ambos fabricantes encadenaría una cascada de demandas y recursos. En una primera vuelta la surcoreana perdería, condenada a una indemnización de 1049 millones de dólares que pasarían a 450 en una siguiente ronda por parte de la misma juez, Lucy Koh, al querer precisar más las cifras reclamadas. Poco después se ampliaran los casos y se incluirán nuevas patentes, en un torrente de cuestiones cada vez más abstractas y difusas y un aluvión de nuevos productos, que recurrentemente se aportaban con cálculos coincidentes con las campañas navideñas[358].

Apple terminaría demandando a las siete principales compañías que empleaban el sistema operativo Android. Como reacción, Google acudió al respaldo de todas estas, poniendo a su disposición toda la remesa de patentes de la que era poseedora. En principio de forma no declarada, aunque luego, una vez parte de las demandas, como parte interesada[359].

La compra millonaria de Motorola por parte de Google, cuando no su estrategia en lo que respecta a la tecnología móvil era precisamente que sus dispositivos *Nexus* (dispositivos avalados por Google) fueran fabricados por diversas marcas que apoyan Android debe entenderse como una manera de tratar de hacerse con la cartera de patentes de la compañía, precisamente en un momento en que debía encarar el proceso abierto por

---

[358] La publicación The Verge, hizo un seguimiento detallado de los juicios y recopiló las patentes argüidas en los diferentes casos: http://www.theverge.com/2012/7/30/3199424/apple-vs-samsung-trial-guide/in/2971889

[359] Enrique Dans. *La verdadera razón del Juicio de Apple contra Samsung*: http://www.enriquedans.com/2012/11/la-verdadera-razon-del-juicio-apple-vs-samsung.html

Apple. La posterior venta de Motorola, reteniendo las patentes, así lo dejaría evidenciado.

La realidad es que buena parte de estas demandas se sustentaban en usos bastante genéricos e incluso en aspectos relativos a la imagen, que como dispositivos convergentes que son, no podían, menos aún en sus inicios diferir en gran medida en los que a su función se refiere. En muchos aspectos, buena parte de la innovación que defendía Apple no era tal. Tan solo conocer a fabricantes como HTC, con una trayectoria dilatada en dispositivos tipo Smartphone con el fallido sistema operativo Windows Mobile, en el mercado más de un quinquenio antes de la aparición del primer iPhone, nos puede ubicar en el contexto de toda la campaña.

Con cierta perspectiva y atendiendo a los resultado finales, queda claro, aparte de las fijaciones personales de Jobs, que la ofensiva legal sirvió a Apple para jugar un doble juego en EEUU, primero como pieza clave de un tablero geopolítico, en el que ganarse las simpatías más nacionalistas frente a empresas extranjeras (aunque sus productos los fabriquen los mismos chinos en las factorías de *Foxconn*) y por otro lado jugar una estrategia de dilación en la que demorar los lanzamientos de productos estrella de la competencia para retrasar el desplazamiento de su hegemonía, en el sector de las tabletas principalmente. Si atendemos a esos resultados, la campaña resultó un éxito dado que ambos objetivos fueron cubiertos sobradamente y el acuerdo final de no continuar los procesos termina por avalar esta teoría.

Los Trolls de las patentes

El fenómeno del denominado "Troll de las patentes", empresas dedicadas a la gestión de patentes para plantear litigios de los que extraer beneficio económico, son un fenómeno genuinamente norteamericano, surgido al calor de la "mano laxa" de la oficina de patentes de dicho país en lo que respecta a la inscripción en su registro. El neologismo hace referencia a estos grupos que no producen ni buscan otra cosa que atacar a quienes inician un proyecto empresarial cuando pueden "demostrar" el uso de una de sus patentes. Por lo tanto, podemos señalar que la actividad principal de estos despachos se enfoca en la extorsión y la amenaza a empresas así como el acaparamiento de patentes para ampliar su base de negocio.

Despachos como *Intellectual Ventures*[360], que ocupa el quinto lugar en el registro de patentes de EEUU, sin tener otra actividad reconocida que la propia gestión de estas patentes es ejemplo paradigmático de como se ha orientado el asunto. Casos como la venta masiva de patentes de una grande de la fotografía como Kodak, ante la crisis en la que esta empresa se encontraba inmersa, seria mediada precisamente por esta para que un grupo de empresas optaran por ellas. En todo ello, el papel de la oficina de patentes de EEUU[361] ha jugado un papel muy permisivo a la hora de dejar pasar registros poco detallados y genéricos que daba pie a demandas bastante peregrinas.

---

[360] Intelectual Ventures, el conocido como mayor Troll de las patentes de EEUU.http://www.intellectualventures.com/

[361] Oficina de patentes de EEUU: http://www.uspto.gov

Nombres como Soverain Software, *Lumen View Techonology, Rockstar, Rembrandt IP* o la citada *Intellectual Ventures,* solo aparecen en las ocasiones en las que las disputas por las patentes llegan a los tribunales estadounidenses (animo a que se busquen en la red). La situación ha llegado a un límite en el que el senado de EEUU ha optado por establecer un nuevo marco legal en discusión desde 2014 a propósito del camino tomado por las disputas por patentes. Mientras tanto, algunas sentencias judiciales han tratado de mitigar el efecto de estas demandas con argumentos en contra de las patentes sobre ideas[362], a pesar de los cual con datos de 2014, el incremento de estas demandas había adquirido un crecimiento exponencial respecto a la pasada década [363] . El mayor problema de este debate es que el sistema de patentes con el que cuentan es parte esencial de la estrategia de mercado de muchas de las grandes empresas del sector tecnológico, hasta tal extremo que lidiar con estos despachos dedicados a la extorsión legal llega a ser considerado un mal menor, si se pondera frente a su estrategia competitiva, en la que precisamente las patentes juegan un papel relevante. Así se puede entender cómo Microsoft sea uno de los grandes beneficiarios del sistema operativo Android, tras un acuerdo de cesión de patentes que le reporta unos 2000 millones de dólares anuales[364]. Por otra parte, universidades y empresas han focalizado parte de sus investigaciones en la obtención de patentes y el panorama ha llegado a desdibujarse hasta tal extremo que

---

[362] Reportaje *de ArsTechnica* sobre el incremento de los litigios por patentes hasta el año 2014: http://arstechnica.com/tech-policy/2014/05/the-year-in-patent-litigation-more-trolling-more-texas/

[363] Sobre algunas sentencias que tratan de mitigar los efectos de patentes sobre ideas en la revista *Wired*: http://www.wired.com/2015/02/patent-wars-may-cooling-theyre-far/

[364] *Bussines insider* nos explica los 200.000.000$ que consigue Microsoft por el uso de patentes a diversos fabricantes de dispositivos Android: http://www.businessinsider.com/microsoft-earns-2-billion-per-year-from-android-patent-royalties-2013-11

resulta muy complicado trazar un ámbito que satisfaga a las partes y reduzca la "*litigiosidad*" del sistema.

Este fenómeno, junto con el precedente de las demandas iniciadas por Apple, llevarían a un conjunto de compañías estadounidenses, entre las que destacan firmas como Google, Facebook, Zynga, Intuit, Rackspace, Homeaway, y Red Hat a crear un grupo de estudio e influencia para evitar el registro de patentes abstractas, que puedan luego ser empleadas para sacar beneficios de estas empresas. El lastre del sistema de patentes en el sector tecnológico y de Internet, comenzó a pesar demasiado incluso para las grandes compañías del sector, que ven como parte de sus fondos han de ser desviados de forma recurrente en cuestiones legales o en la adquisición de patentes tan solo para proteger su negocio[365] .

Las consecuencias de estas prácticas suponen un freno a la innovación, dado que someten a muchas empresas a la extenuación de recursos para evitar o encarar diversos procesos judiciales frente a los que muchas PYMES no pueden estar preparadas. Esto deja cada vez más expedito el terreno a la gran empresa que acapara recursos y adquiere a muchas de estas compañías amenazadas. Si a esto añadimos la política de adquisiciones y concentración de las grandes empresas tecnológicas y de Internet, vemos como el "ecosistema" empresarial comienza a simplificarse en torno a muy pocos actores. Por suerte, esa laxitud en el registro de patentes y la amplia capacidad de registrar elementos apenas con documentos eminentemente descriptivos, no se ha impuesto en

[365] En 2011 Google, Facebook, Zynga, Intuit, Rackspace, Homeaway, y Red Hat, iniciarían una campaña unida contra las patentes abstractas: http://es.scribd.com/doc/116141978/TechCrunch-Google-Facebook-Amicus-Brief-Criticizing-Patents-On-Abstract-Ideas#scribd

Europa, aunque parte de estas disputas se han producido en este territorio en ningún momento han llegado al alcance estadounidense.

La crítica al sistema de patentes y la petición de su acotamiento o supresión está en el debate de colectivos cívicos y de defensa del Software Libre. La conclusión de que en la actualidad son mayores los perjuicios que los beneficios y que la simple ventaja de ser pionero ya es suficiente en un entorno competitivo sin necesidad de más restricciones. El ámbito biomédico, sin ser tema de nuestro trabajo, es otro de los terrenos donde la crítica del sistema actual de patentes mantiene los mayores debates [366].

Como conclusión, vemos como en el terreno tecnológico, las patentes han servido como instrumento competitivo, empleado como palanca para asegurar monopolios y cerrar puertas a cualquier posible competencia. Desde diversos ángulos, las grandes empresas del sector tecnológico y de Internet, se han entremezclado en una colisión de intereses en las que la legislación, tanto por el poder de otros sectores como por la inercia histórica de un sistema que forma parte del propio sistema económico, ha jugado a favor de los que desde una posición de predominio puede acaparar mayor número de registros. Todo ello abunda en un proceso de concentración en el que las posibilidades de ascenso de nuevos actores son prácticamente marginales, incluso entre los denominados "unicornios"[367]. En definitiva el sistema de patentes, supone

---

[366] . La ONG, *No Gracias*, ha elaborado una fuerte crítica a la utilización de las patentes por parte de laboratorios europeos y estadounidenses: http://www.nogracias.eu/2014/11/16/el-fracaso-de-las-patentes/

[367] Véase 2.6 La red como mercado de burbujas, en donde detallamos el intinerio de inversiones de lo que hoy son las grandes de internet y el surgimiento de lo que se ha definido como “unicornios”(empresas con una capiltalizacion superior al millón de dólares)

la adecuación de los monopolios a una libertad de empresa trucada en el que la innovación es un valor en venta y un terreno de disputa[368]. El sistema de patentes, como clave y contradicción del propio sistema económico se ha convertido en un absurdo que lastra la innovación, al bloquear el acceso a ciertos estándares sobre los que la industria debería trabajar y causan un perjuicio social que solo sirve como instrumento monopolista[369].

[368] Michele Boldrin y David K. Levine*: Against Intellectual Monopoly*:http://www.dklevine.com/general/intellectual/againstfinal.htm

[369] Documental realizado por la comunidad ligada a la FSF sobre el absurdo de las patentes en los terrenos del software y la innovación tecnológica: http://patentabsurdity.com/

3.6 GNU, Software Libre y CopyLeft frente al mercado y mercantilización cultural.

Desde el punto de vista comercial, de una forma mercantilizada de entender la cultura y la creación, el software libre se ha convertido en una de las formas de expresión cultural a combatir con una fiereza desproporcionada por parte de las grandes corporaciones poseedores de grandes nichos de mercado, en muchas ocasiones monopolios en la práctica que ven en este tipo de planteamientos un enemigo radical a su forma de negocio.

El planteamiento original, de una forma colaborativa y abierta de entender la creación de aplicaciones informáticas ha conseguido con el tiempo remover buena parte de los obstáculos mediante un sentido de "comunidad de la información". Esta visión otorga al usuario el control completo de las tareas, frente al software privativo, en el que hay que someterse al marco de la licencia sin posibilidades de mejora, copia, estudio o edición [370]. Por ello, el conflicto entre software libre y las empresas dedicadas a la distribución y venta de software privativo es uno de los terrenos de mayor disputa entre extremos de un mismo entorno. A pesar de ello, la realidad es siempre compleja y está llena de matices y grados. Por un lado veremos a lo largo del presente punto y del siguiente cómo no son solo activistas y grupos comprometidos los que defienden el software libre sino que estados y empresas de diversos subsectores de lo

[370] Stallman, R. *Software Libre para una sociedad libre*. Traficantes de sueños Ed. Madrid. 2013. Edición electronica: http://www.traficantes.net/libros/software-libre-para-una-sociedad-libre

tecnológico apoyan o se identifican con este por interés propio, incluso animando la creación de comunidades en torno a productos o desarrollos patrocinados o colaborados[371]. Casos como el apoyo financiero inicial de Google a Mozilla Firefox, de la fundación Mozilla[372], para luego lanzar su propio navegador, Google Chrome, basado a su vez en el navegador de código abierto *Chromium*[373], con una comunidad propia de desarrolladores a la que anima para implementar mejoras en su propia opción, de la que saca partido, son ejemplo de cómo una comunidad de desarrolladores puede terminar sirviendo de apoyo a una gran empresa.

Las políticas de cierre de ciertas empresas en lo que respecta a su software han tenido una trayectoria desigual. Mientras que a Apple, con un control férreo de sus productos, tanto de hardware como de software, le ha funcionado bien como marca porque su estrategia de marca y los márgenes de sus productos se lo permiten, casos como el de Sony no han cesado de chocar contra comunidades de usuarios y hackers por el cierre y el cambio de políticas respecto a sus productos, vendidos originalmente con unas condiciones que luego cambiarían unilateralmente perjudicando multitud de desarrollos como los que estaban produciéndose en torno a su consola *PlayStation 3*[374] . Como veremos, tanto en un caso como en otro, diversos usuarios conseguirían remover los obstáculos de estas compañías a la modificación de sus productos, entablando un terreno

---

[371] Kleim, N. No logo*. El poder de las marcas*. Booket. Madrid. 2011

[372] La Fundación Mozilla, sin ánimo de lucro, cuenta con el navegador Firefox como producto estrella: https://www.mozilla.org/es-ES/about/

[373] El Proyecto Chromium: Una comunidad de Software libre patrocinada por Google: https://www.chromium.org/

[374] *La guerra de los gigantes de internet*. Artículo de *Businness Insider* sobre el conflicto de intereses de las grandes empresas de internet: http://www.businessinsider.com/apple-google-amazon-facebook-war-2012-12

de disputa en el que la opción por los desarrollos libres se verá cada vez como el camino más razonable y adecuado[375].

El movimiento del software libre

A lo largo de los años '60 y '70 del pasado siglo, partimos de un modelo informal, que en sus orígenes distribuía el código fuente de sus sistemas operativos, como el caso de IBM con sus sistemas *mainframes* (grandes servidores). El aumento del costo de programación, de la mano de sistemas cada vez más complejos llevaría a restringir el acceso a sus creaciones a una potencial competencia. Los programadores, ya no podían intercambiar el producto de su trabajo realizado dentro de sus empresas. La misma AT&T, distribuía su sistema operativo UNIX entre investigadores y gobiernos de forma gratuita pero impidiendo cualquier modificación por parte de estos. Este será el comienzo del software privativo y el primer origen de la búsqueda de alternativas[376].

El movimiento por el Software Libre comenzaría en 1983, de la mano de una de las figuras más carismáticas del activismo en la red, Richard Stallman, que definiría el inicio de un sistema GNU basado precisamente en UNIX y una comunidad destinada a desarrollar toda la tarea, denominada la *Free Software Foundation*[377] . Si bien es cierto que

---

[375] VVAA. *Internet y Lucha política: Los movimientos sociales en la red*. Capital Intelectual, Buenos Aires, 2006

[376] Manuel Castells. La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad. Plaza & Janes. Barcelona. 2001

[377] . La definición de GNU y la documentación al respecto puede encontrarse en la web del proyecto: https://www.gnu.org/home.es.html

no serían la primara comunidad que compartiría el producto de su investigación, solo tenemos que remitirnos a la misma gestación de Internet, será la primera ocasión en la que establecerán una estructura y unos principios. Una toma de conciencia política en cierta medida de su importancia y la implicación de sus decisiones en el terreno turbulento de la disputa comercial en la que Windows comenzaba a imponerse en el mercado[378] .

Uno de los grandes logros de la comunidad de software libre sería la de conjugar cierto número de trabajos dispares dentro de un proceso confluyente. Así en 1990, se disponía de la mayor parte del sistema operativo a excepción de un núcleo solvente sobre el que implementarlo. Casualmente en 1991 el finlandés Linus Torvalds, programaría por su cuenta un núcleo de sistema para poder trabajar en casa sobre un UNIX no restringido. En agosto de 1991, Torvalds escribió en el grupo de noticias *comp.os.minix* (dedicado a GNU) sobre el sistema que estaba desarrollando[379] . Tras esta explicación, recibirán mucha ayuda de la comunidad de software libre hasta conseguir un mes más tarde tener lista la primera versión de dicho núcleo.

---

[378] La historia de GNU: http://www.gnu.org/gnu/gnu-history.es.html

[379] Sobre Torvads y el tablero de GNU. Este es el texto que escribiera en el grupo de noticias *comp.os.minix:*

"Estoy haciendo un sistema operativo (gratuito, sólo un hobby, no será nada grande ni profesional como GNU) para clones AT 386(486). Llevo en ello desde abril y está empezando a estar listo. Me gustaría saber su opinión sobre las cosas que les gustan o disgustan en minix, ya que mi SO tiene algún parecido con él. [...] Actualmente he portado bash(1.08) y gcc(1.40), y parece que las cosas funcionan. Esto implica que tendré algo práctico dentro de unos meses..."

Stallman lo convencería en 1992, para que lo publicara bajo licencia GPL (Licencia Pública General) [380] , modificable pero solo distribuible bajo la misma forma. Con ello, se tenía la base de un sistema operativo solvente y alternativo: Linux.

A la hora de definir el software libre, suele ser común mencionar las cuatro libertades con el que el proyectivo GNU define su campo. La *libertad 0,* de ejecución el programa a discreción, la primera, de estudiarlo y adaptarlo según necesite, la segunda, de distribuir copias y la tercera, de mejorar y publicar estas modificaciones a toda la comunidad. Para que todos estos aspectos puedan aplicarse en acceso al código fuente, la escritura base del programa es un requisito esencial. Precisamente, el aspecto de libertad como un concepto que supera la idea de lo mercantil, pero que no significa impedir el negocio. Dicha idea también es remarcada por sus creadores al ser *Free* un término menos específico que en castellano, que diferenciamos entre *gratis* y *libre*[381]. Los cuatro puntos de la licencia GPL (General Public License) tendrán una influencia que trascenderá el ámbito del software, para adquirir, en cierta medida el carácter de manifiesto. Una declaración de intenciones en pos de la libertad personal en el nuevo ámbito tecnológico de nuestro tiempo con una influencia que veremos cómo transciende el ámbito del software[382].

---

[380] . Sobre la licencia GPL su texto al detalle: http://www.gnu.org/licenses/lgpl.html

[381] VVAA. *Cultura Libre Digital*. Icaria. Barcelona. 2012

[382] Las cuatro libertades esenciales de software expresadas por la FSF son:

- *La libertad de ejecutar el programa como lo desee, con cualquier propósito (libertad 0).*

El movimiento y el propio carácter de su fundador, tiene una clara identidad política, aunque esta no siempre sea declarada de forma abierta. En general el argumentario oscilaría entre la izquierda transformadora, en la que el mismo Stallman milita (pertenece al partido verde estadounidense)[383] y ciertas prácticas de carácter libertario. La efervescencia de la propia comunidad y la traslación de acciones hacia contextos más politizados, ya sea en la militancia pro derechos civiles como hace la EFF, en defensa de las libertades en la red, que alcanzaría su máximo punto de tensión con la persecución de Aaron Swatrtz[384] y su posterior suicidio , o ya sea hacia una actividad más dedicada al hacking militante, como harían grupos autodenominados Anonymous, o Lulzsec entre otros, cuestiones que trataremos en sucesivos capítulos, será una de sus características más extendidas[385]. La progresiva politización de

---

- *La libertad de estudiar el funcionamiento del programa y adaptarlo a sus necesidades (libertad 1). El acceso al código fuente es un prerrequisito para esto.*

- *La libertad de redistribuir copias para ayudar a los demás (libertad 2).*

- *La libertad de mejorar el programa y de publicar las mejoras, de modo que toda la comunidad se beneficie (libertad 3). El acceso al código fuente es un prerrequisito para esto.*

[383] El Partido Verde de los Estados Unidos, conseguiría unos resultado muy destacables en las campañas de 1996 y 2000, en las que Ralf Nader sería su candidato: http://www.gp.org/

[384] *The Internet's Own Boy: The Story of Aaron Swartz*.: Sobre la historia de Aaron Stwartz Se produjo un documental financiado en la plataforma Kikstarter (https://www.kickstarter.com/projects/26788492/aaron-swartz-documentary-the-internets-own-boy-0) ,que finalmente sería subido a la plataforma YouTube https://www.youtube.com/watch?v=vXr-2hwTk58. También cuenta con una reciente traducción al castellano en https://www.youtube.com/watch?v=czmVVU7uiBc.

[385] VVAA. *Internet y Lucha política: Los movimientos sociales en la red*. Capital Intelectual, Buenos Aires, 2006

algunos sectores hacia una actividad concreta sin embargo, no ha conseguido, salvo casos puntuales, como el Partido Pirata sueco[386], llegar a acoger a toda la comunidad en la que la dispersión es una característica fundamental de un movimiento deslocalizado, aunque muchos de sus miembros más ligados al activismo social ya tienen una identidad colectiva clara[387].

En la actualidad el modelo de software libre y su extensión a lo largo de múltiples tipos de licencias[388] han permitido el desarrollo de muchos de los avances tecnológicos de los últimos años. El núcleo de Linux está presente en multitud de servicios desde servidores empresariales hasta los móviles Android, pasando por multitud de dispositivos que mediante diversas variaciones lo implementan. El propio movimiento ha tenido una influencia fundamental en la gestación de otras comunidades y proyectos libres como las licencias *Creative Commons* o *CopyLeft*, extendiendo la misma filosofía a los mundos de la creación artística y proyectos como la Wikipedia o fundaciones como Mozilla. A partir de estos movimientos, se han comenzado a sistematizar respuestas colectivas al modelo económico y social trazado con el nombre de la nueva economía, por parte de empresas y gobiernos identificados con estas, al ir apareciendo mayor número de puntos de conflicto y contradicción. El hecho de que nuevas identidades y formas de acción terminen por asentar un debate superior sobre los modelos económicos y sociales será un punto de inflexión cuyo alcance todavía está por determinar pero que ya es un

---

386 *Partido Pirata sueco*, el primer partido que sistematizó un ideario de libertades digitales y lo concretó en una opción política: http://www.piratpartiet.se/

387 VVAA. *Cultura digital y movimientos sociales*. Catarata. Madrid. 2008

388 Una proyección gráfica sobre las licencias libres más empleadas en la actualidad: https://www.blackducksoftware.com/resources/data/top-20-open-source-licenses

agregado al resto de movimientos sociales existentes en nuestra sociedad y como tales, merecen una consideración y análisis para poder conocer la sociedad de nuestro tiempo[389].

Las Comunidades de investigación y desarrollo en Internet frente a la gran empresa.

El desarrollo de comunidades o grupos de usuarios interesados en mejorar, ampliar o investigar sobre diversos aspectos de software o hardware son uno de los ejes principales en la expansión del Software libre. De cualquier modo no todas las comunidades han transparentado su actividad e incluso existen foros dedicado a plataformas concretas de las que parten tanto desarrollos libres como privativos. En los últimos tiempos estos foros han servido de escaparate para una política de fichajes de ingenieros y desarrolladores por parte de la gran empresa del medio.

En ese sentido, tenemos uno de los ejemplos de mayor referencia en *XDA Developers* [390] Dicho foro, inició su andadura en 2003, dedicándose primero a dispositivos móviles del momento, sobre todo con sistemas operativos *PalmOs* y *Windows Mobile* y los primeros navegadores GPS. Desde ese momento, muchos desarrolladores, como

---

[389] . Lessig.L. *Por una Cultura libre*. Cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad. LOM. Santiago, 2005. Edición electronica: http://www.traficantes.net/libros/por-una-cultura-libre

[390] El foro XDA Developers es en la actualidad una de las mayores influencias en el sector tecnológico de la telefonía móvil en general. El trabajo de sus usuarios y el peso de sus debates han llegado en ciertas ocasiones a hacer cambiar de idea a ciertos fabricantes, ante la perspectiva de que la comunidad proponga acciones de boicot contra estos: http://www.xda-developers.com

ModaCo o Chainfire, comenzarían a implementar mejoras en los dispositivos para mejorar su usabilidad. Muchas de las mejoras aportadas en estos foros, eran en principio rechazadas por los fabricantes, incluso declarando ilegal la intervención en sus equipos. Con la llegada de *iOs y Android*, se alcanza la verdadera expansión del foro. La posibilidad de desbloquear los primeros iPhone (el famoso Jailbreak), para aprovecharse de mejoras creadas por aficionados del foro, llevaría a una lucha legal por parte de Apple contra diversos usuarios. Por otra parte, las posibilidades Android, un sistema que es parcialmente propietario de Google que es quien desarrolla las sucesivas versiones para luego ser sucesivamente liberadas a la comunidad, permitieron desbloquear los terminales, adquirir permisos de administrador (root) y poder cambiarle incluso la ROM del sistema (el sistema operativo al completo)[391]. A partir de ese momento, una multitud de creadores de software y técnicos en hardware, crearían aplicaciones para tomar el control completo de los terminales más populares y mejorarlos al completo[392]. Asimismo, se comenzaron a desarrollar versiones completas del SO Android totalmente desligadas de Google. A estas derivaciones se les conoce como Forks. *CyanogenMod* será una de las más famosas y extendidas.

En principio, la discusión de si Android es libre realmente o es un instrumento de Google para colocar sus servicios en una serie de empresas implicadas en la *Open Handslet Aliance*[393], fuente teórica de los

---

[391] Reischl, G. *El engaño de Google*. Medialive Content. Barcelona. 2008

[392] Respecto a la importancia de un sistema operativo abierto, he escrito varias colaboraciones en medios tecnológicos. Una de las más destacadas es esta: Los dispositivos móviles, entre la libertad y el interés comercial: http://www.eldiario.es/turing/dispositivos-moviles-libertad-interes-comercial_0_117938633.html .

[393] *Open Handslet Aliance*. La confluencia de fabricantes y empresas tecnológicas para la consecución de estándares comunes en la tecnología móvil y cuyo mayor trabajo es

sucesivos desarrollos. Ciertamente, Android se ha liberado en todas sus versiones mediante licencia Apache[394]. La clave está en el control de compatibilidad, una forma en la que Google, propietaria de la "marca" Android, da su visto bueno a los fabricantes, con la excusa de evitar la *fragmentación* del sistema operativo. Este visado de "compatibilidad" con el AOPS (Android Open Source Project) se obtiene precisamente cumpliendo con la documentación de compatibilidad y pasando el test citado. Por tanto, aunque se libere con licencia Apache, que no revela nada más que la parte del código que está obligada al derivar del núcleo Linux, Google mantiene un control bastante estrecho de las versiones. Asimismo, los fabricantes no liberan la parte que les corresponde de los controladores de sus dispositivos y también se han dado casos de inclusión de código malicioso, como el caso de Carrier IQ[395], que se insertaba de forma oculta para enviar información de los usuarios de los dispositivos. Stallman va más allá, recurriendo al caso de Carrier IQ, al afirmar que las partes no liberadas de Android e iOs en su conjunto deben ser consideradas como malware (software de código malicioso para espiar a usuarios). Esto llevaría a una campaña por la liberación de los dispositivos Android, que tiene margen para hacerlo, con versiones totalmente libres y transparentes y aplicaciones no propietarias ni dependientes de ninguna gran compañía[396]. Como veremos, los sucesivos escándalos sobre la vigilancia masiva de usuarios filtrados por WikiLeaks o Edward Snowden, abundarán aún más en lo explicado.

Android. : http://www.openhandsetalliance.com/index.html

[394] Sobre la Licencia Apache: http://www.apache.org/licenses/LICENSE-2.0.html

[395] Sobre el Software Espía Carrier IQ Incluido por algunos fabricantes y operadores estadounidense: http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/

[396] Campaña de la FSF para mantener tu móvil Android Libre: http://fsfe.org/campaigns/android/liberate.es.html. La versión en inglés se mantiene más actualizada en: http://fsfe.org/campaigns/android/liberate.en.html

La extensión de versiones no controladas por Google del Android original, se han ido multiplicando. Google no ha escatimado en descalificar las modificaciones de un producto sobre el que vuelca importantes recursos y que ha sido una de sus estrategias comerciales claves de la última década[397]. Más que sobre desarrollos libres, que buscan el control por parte de sus usuarios de todo el proceso que corre sobre sus terminales, como Replicant[398], AOPK[399], OmniRom[400] o CyanogenMod[401], entre los más destacados, Google ha sido incapaz de poner coto a versiones con una clara orientación comercial fuera del ecosistema de la compañía como el caso de *Fire OS*[402] , que implementa Amazon en sus terminales y tabletas junto con su propia tienda de aplicaciones, o los desarrollos chinos, que también prescinden de toda relación con la gran G y sustraen por tanto a todos sus usuarios del uso de sus aplicaciones y servicios, como hacen fabricantes como Xiaomi, con su Miui ROM[403] o Baidu Yi[404], de la empresa Baidu, el gran monopolio chino de las búsquedas y los servicios en línea. Con el tiempo, grupos como el de Cyanogen, terminarían por pasar al mundo comercial siendo la instalación por defecto de nuevas compañías de terminales chinos de calidad. Esta proliferación de Forks[405], que sitúan

---

397 Los miembros de GNU también discute sobre la libertad de Android y su control por parte de google: http://www.gnu.org/philosophy/android-and-users-freedom.es.html

398 Replicant, la versión segura y transparente de Android: http://www.replicant.us

399 AOKP (Android Open Kang Project) http://aokp.co

400 OmniRom: http://omnirom.org

401 CyanogenMod: http://www.cyanogenmod.org

402 FireOs: https://developer.amazon.com/appsandservices/solutions/platforms/android-fireos

403 MIUI: http://en.miui.com

404 Baidu Yi http://os.baidu.com

405 Artículo de *Mobilforge* sobre los Forks de Android y la posición de Google al respecto:

a Google fuera del sistema operativo que apadrina, a terminado por ser considerado como un mal menor por la compañía, que finalmente sigue siendo la que controla ciertos aspectos y la mayor parte de la masa de usuarios y fabricantes. Precisamente el aspecto cerrado de ciertos recursos de su sistema acapara las críticas más virulentas, sobre todo a la vista de los sucesivos problemas de seguridad y la acción de las grandes empresas tecnológica que tan solo evita parcialmente los sucesivos escándalos[406].

En la que ya muchos denominan la era post PC, dado los grandes consumos que otros tipos de dispositivos hacen de la red, la carrera por posicionarse en la ventana de inicio del usuario se ha convertido en una carrera en la que el dominio de la plataforma resulta vital para las grandes empresas. Al igual que para navegar son todavía una cantidad muy destacada de usuarios los que realizan una búsqueda con google, aunque sepan dónde quieren ir, apoderarse del dispositivo de acceso significa potenciar los ingresos de la empresa que lo consiga[407]. Por ello, para Google, su tienda de aplicaciones, Google Play Store (que también vende libros, música y películas) junto con su buscador y su ecosistema preinstalado en todos los Android reconocidos como "compatibles" es la clave y no tiene reparos en suspender aplicaciones o dificultar la instalación desde fuentes externas, aunque estas sean libres y se ofrezcan en

https://mobiforge.com/news-comment/android-forks-why-google-can-rest-easy-for-now

[406] Richard Stallman sobre la consideración como malware de los sistemas operativos cerrados: http://www.techtimes.com/articles/55532/20150527/malware-all-malware-how-free-software-advocate-richard-stallman-sees-windows-android-and-

[407] Suárez Sánchez Ocaña, A. *Desnudando a Google*. Deusto. Madrid. 2012

mercados alternativos como FDroid[408]. Casos Como el de Adaway[409], que bloquea la publicidad con filtros propios, no controlados por Google, son ejemplares. La estrategia es compartida por Apple, con su tienda Apple Store (puerta a su ecosistema) y por Amazon, que enlaza su tienda de aplicaciones con su apuesta editorial. Los que se ven fuera de ello, como Facebook, lo intentan integrando mensajería con un portal y un servicio de noticias integrado que haga que los usuarios no salgan de su ecosistema. Lo principal es permanecer el mayor tiempo posible dentro de aplicaciones y servicios de la marca. El tiempo es "conversión" y parte principal del negocio, ya sea derivado de publicidad o por suscripción a servicios de pago.

En lo que respecta a iOs, el otro gran sistema operativo que se disputa la hegemonía real de los dispositivos post PC, su gestación es mucho más restrictiva, dado que todo el software es propietario y vinculado solamente a los dispositivos de la marca Apple. Por tanto, el cierre es completo y aunque se trata en esencia de un derivado de Unix, que comparte mucho en común con el propio Android, tanto su sistema como el propio hardware del dispositivo es completamente cerrado. Todo ello no significa que no se pudiera en su momento tener acceso administrativo del dispositivo y desbloquearlo. Sucesivas versiones del famoso *Jailbreak* (el método de explotar una vulnerabilidad que da paso al desbloqueo del terminal). En su momento, Apple trataría de declarar incluso ilegal el proceso en sus dispositivos, aunque tras un largo debate legal, con una fuerte campaña en contra por parte de grupos de derecho como Freedom

---

[408] En *FDroid*, se ofrecen múltiples aplicaciones Libres, muchas de estas noc disponibles en las tiendas "oficiales" por tener características que no son del agrado de Google:https://f-droid.org/

[409] *Adaway* es una de las aplicaciones que no son del agrado de Google, al bloquear publicidad y ofrecer al usuario de Android la libertad de configurar sus litas blancas y negras: https://sufficientlysecure.org/index.php/adaway/

House o la EFF[410], no sería esa vía la que pudieran emplear para el cierre. El paso más recursivo ha sido el lanzamiento de actualizaciones OTA (Over The Air) que se instalan de forma sencilla y bloquean el acceso de cada uno de los procesos de investigación[411].

La primera persona en conseguir desbloquear los primeros iPhone y alcanzar acceso ampliado al dispositivo sería un adolescente de 17 años llamado Georg Hotzen 2007. En una noche, conseguiría abrir el dispositivo, establecer una pequeña soldadura con la que conectar a su ordenador el dispositivo y lograr extraer la Banda Base (BaseBand), sobre la que operar a continuación. En un vídeo grabado en la cocina de su casa, mostraría el primer iPhone desbloqueado de la historia. El vídeo se haría inmediatamente viral y *Geohot* (su sobrenombre en la red) alcanzaría la fama[412]. Steve Wozniak, el auténtico corazón del sistema operativo Apple y que tanto cuestiona en la actualidad el rumbo de la empresa felicitaría en su momento a Geohot por conseguir desbloquear los primeros iPhone, Su ejercicio de ingeniera inversa, conseguiría no solo el desbloqueo de los terminales sino la posibilidad de mejorarlos con implementaciones de software [413], como las que introduce *Cydia* (que recibe su nombre irónicamente del gusano de la manzana) que Apple tardaría años en introducir, como el caso de los menús desplegables, ya activo vía

---

[410] La EFF archiva mucha información sobre el caso. En su momento, se mantuvo muy activa frente a Apple: https://www.eff.org/press/archives/2010/07/26

[411] Apple sigue tratando de advertir sobre el Jailbreak y amenaza con la pérdida de garantía: https://support.apple.com/es-es/HT3743

[412] El vídeo en el que *Geohot* muestra su primer iPhone desbloqueado: https://www.youtube.com/watch?v=tvJ1RGIxe8Q

[413] En una entrevista, años más tarde,Hotz habla sobre el desbloqueo de los "idevices": https://www.youtube.com/watch?t=47&v=uvAfKJm-exw

Jailbreak en 2007. En este sentido, Apple, en nuestros días sigue cerrando sus sistemas y los recurrentes Bugs (fallos del sistema) que son explotados para desbloquear sus máquinas, son recurrentemente parcheados. La clave en la celeridad de Apple por cerrarle el paso a estas implementaciones, es la posibilidad de instalar cualquier aplicación sin tener que pasar por su tienda, no solo piratas sino editadas libremente por programadores independientes. Si bien es cierto que un fallo puede vulnerar al sistema, la realidad es que la amenaza de introducción de un mercado alternativo de aplicaciones es una gran preocupación y acicate de estas actualizaciones.

El tercer gran caso, por su notoriedad, en lo que respecta a las disputas entre comunidades de usuarios y grandes empresas del medio tecnológico nos llegara con la consola de videojuegos PlayStation 3, de la multinacional Sony. En su lanzamiento, dicho aparato contaba con una potencia importante y una relación precio- capacidad muy interesante. La posibilidad de instalar versiones adaptadas de Linux haría que usuarios e incluso investigadores la emplearan como máquinas con diferentes enfoques. Realizar un *clúster* (un enlazado de máquinas para que trabajen como un potente servidor) con estas, era una posibilidad que muchas universidades y laboratorios explorarían. Esta opción, no excluía que, a diferencia de su predecesoras, tan fácilmente desbloqueables para jugar con copias de juegos, no estuviera desbloqueada, tan solo permitía un gestor de arranque abierto mediante el que se tenía la posibilidad de ejecutar un sistema operativo Linux (derivado de la conocida distribución Debian). Todo esto desaparecía de la mano de la primera tanda de actualizaciones mediante la que Sony pretendía que todos los usuarios se mantuvieran conectados a su *Play Station Network* (PSN), con

in identificador (Id) personal único y ligado a cada máquina[414]. Un enfoque hacia los contenidos que ya conocemos de otras empresas y que Sony quería fundamentar alrededor de su producto de consumo estrella.

De nuevo Geohot[415] sería una pieza fundamental del puzle. Tras las polémicas actualizaciones en las que Sony, impedía todos los usos alternativos de la consola, el hacker se planteó que ya era tiempo de investigar la Playstation3 y desbloquearla (llevaba tres años en el mercado e ese momento). Para una comunidad de usuarios ya movilizada por la arbitrariedad de la empresa, la llegada del primer *Custom Firmware* (nombre del primer sistema de desbloqueo de la consola) será acogida de forma masiva a lo largo de 2010. La reacción de Sony será la de iniciar un proceso legal contra Geohot[416] y el bloqueo (denominado *baneo*) de todos los usuarios que conectaran sus consolas liberadas a la red de PSN. En 2011, Sony ganaría parcialmente el primer juicio prohibiendo la difusión del método[417]. Aun así, otros usuarios menos conocidos, publicarían sucesivas versiones del firmware adaptado para ejecutar aplicaciones Homebrew *(caseras)* para contrarrestar las actualizaciones que publicara Sony y que en ciertas ocasiones impedían el acceso a partidas o la conexión a red, para obligar a los usuarios a realizarlas. Otra reacción paralela será la de Anonymous[418], el colectivo de hackers que bajo esa denominación común,

---

414 La *PSN* de Sony, trata de mantener un control de usuarios mediante in sistema de identificación personal. http://es.playstation.com/ps3/support/

415 Actualmente su web ha retirado sus anteriores referencias a sus "hazañas": http://geohot.com/. Sin embargo, desde Archive.org podemos acceder a la versión histórica de su página en la que se puede leer su estado original

416 *ArsTechnica* ha seguido el caso sobre el Jailbreak de PlayStation: http://arstechnica.com/gaming/2015/04/us-government-takes-on-legal-fight-over-console-jailbreaking-once-more/

417 La truculenta historia dela demanda de Sony a Geohot y el acuerdo final. http://www.newyorker.com/magazine/2012/05/07/machine-politics

418 La operación contra Sony y el intercambio de información sería después copiado a

nacida del foro anónimo *4Chan* (en el que todos los usuarios se llaman Anonymous si no ponen otro nombre)[419]. Desde Anonymous, se iniciaran los primeros ataques DDoS (denegación de servicio o saturación de una página o servidor hasta dejarlos inoperativos), reivindicando la figura de Geohot en contra de la actitud de la compañía Sony. El boicot a la empresa de la *#OpSony* (nombre de la campaña de Anonymous) y las simpatías del caso dañaran la imagen pública de esta. Finalmente se propondrá un acuerdo con Hotz, que negaría la pretensión de usar la consola para la piratería de juegos, mientras Sony retiraba la demanda. Actualmente, sigue siendo posible el desbloqueo tanto de este modelo como de su sucesora la PlayStation 4 [420]. Hotz sería fichado por Facebook y posteriormente por Google.

El desarrollo del Hardware Libre

Como ya hemos tratado anteriormente, Open Compute, el modelo que grandes empresas de la red como Facebook o Google emplean para establecer los parámetros sobre los que se deben basar su infraestructura de servidores ha servido para contribuir a que la escena del hardware se libere de los parámetros cerrados de ciertos fabricantes. El modelo Clásico que podríamos identificar con IBM y muchas de las que disputan la gran clientela, ha sido siempre la de establecer una dependencia de las

Pastebin: http://pastebin.com/JiHQSM74

[419] *4Chan*, es el foro que daría Origen a Anonymous y sus primeras operaciones: http://www.4chan.org/

[420] *PS3Hacks*, el portal que recopila todas las actualizaciones posibles y *Homebrew* disponibles para las consolas de Sony: http://www.ps3hax.net/

infraestructuras y una interrelación de máquinas solamente entre modelos compatibles y desde luego dentro de su ecosistema de marca. Esto significa un lastre a la hora de hacer crecer infraestructuras. El modelo Open Compute, vino a romper este dialogo y cambiar la relación de poder. El cliente gigante, impone la forma en la que deben fabricarse las máquinas sobre las que correrán sus servicios y básicamente estas deberán ser escalables y compatibles. Así será criterios de calidad y competencia los que decidan la elección de nuevos componentes y no el contar con equipos dependientes de ciertos fabricantes. Para ello, incluso la comunicación a bajo nivel de estas tendrá que soportar un estándar reconocido y abierto, analizable y actualizable por parte de la comunidad. Este modelo, por tanto ha supuesto una ruptura cuyas consecuencias todavía no se han transmitido por completo en los modelos de escalas inferiores pero que sin duda, junto con la virtualización de servidores, serán los parámetros que condicionen todos los servicios profesionales.

La capacidad de establecer pautas de desarrollo de dispositivos físicos a partir de los que crear elementos más complejos no es solo exclusiva de la gran empresa. Multitud de investigadores independientes han comenzado a agruparse para establecer una serie de especificaciones comunes y abiertas sobre las que basar cualquier proyecto, con la premisa de que la escalabilidad debe basarse en estándares conocidos. Con esta premisa, nacerá el denominado Hardware Libre[421].

---

[421] Andrades, F. *¿Qué es el Hardware Libre?* :http://www.eldiario.es/turing/Hardware-Libre_0_139986451.html. El artículo tendría interés en su miomento al ser la única fuente en castellano que trataba sobre este movimiento, justo antes de los inicios de la impresión 3D fuera de compañías comerciales y daría pie a varias charlas entre colectivos interesados, especialmente entre *Makers(creadores independietes)* e interesados en el *DiY* (Do it Yorself-hazlo tú mismo).

Durante los últimos años han comenzado a surgir proyectos que pretendía establecer parámetros abiertos para diversos dispositivos con una suerte desigual. Así, ideas como las de los primeros móviles libres, como OpenMoko[422] quedarían abandonadas, mientras que la OLPC (One Laptop per Child- Un ordenador por niño), conseguiría una relativa extensión primero en India o Brasil, y continúa su labor actualmente[423].

Asociaciones como la OSHWA (Open Source hardware Association), tratan de fijar los parámetros comunes para que los desarrollos libres puedan ser extensibles y reconocidos[424]. Las bases sobre las que se establecen los parámetros del Hardware Libre beben del ideario del Software Libre, pero implementado a dispositivos físicos. El primer encuentro de Hardware Abierto, celebrado en Nueva York en 2010, partía de la idea de definir y concretar los principios que deberían darle forma a unas especificaciones genéricas sobre dispositivos libres. La idea partía de una especificación denominada Open Hardware[425], sugerida desde la comunidad de Linux Debian. En 2013 se establecerían los parámetros básicos con los que se guían estos, sobre todo confrontando algunos aspectos legales que ponen trabas al desarrollo de estándares abiertos sobre todo en lo que respecta a patentes. En este sentido, los

---

[422] *OpenMoko*, el móvil GNU que obtuvo poco éxito: http://wiki.openmoko.org/wiki/Main_Page

[423] La campaña OLPC (un ordenador por niño) sigue abierta y ahora mismo trata de extender el acceso a las tecnologías mediante el reparto de tabletas baratas: http://one.laptop.org

[424] OSHWA (Open Source hardware Association). La asociación que pretende definir los parámetros comunes http://www.oshwa.org/definition/spanish

[425] La definición *de Open Hardware* de Debian: https://www.debian.org/OpenHardware/

desarrolladores se han encostrado a lo largo de estos años con multitud de dificultades que han impedido una concreción definitiva[426].

---

[426] Los principios básicos del Hardware libre viene descritos en http://freedomdefined.org/OSHW . Traducidos (no existe actualmente documento en castellano) serían como sigue:

1. ***Documentación:*** El *hardware debe ser puesto en libertad con su documentación completa y debe permitir la modificación.*

2. ***Alcance:*** La *documentación debe especificar claramente qué parte del diseño se publica bajo la licencia.*

3. ***Software Necesario:*** *Si el diseño requiere de licencia de software, este debe cumplir unos parámetros de documentación suficiente y ser publicada bajo una licencia de código abierto aprobada por OSI*

4. ***Obras Derivadas:*** *La licencia debe permitir modificaciones y trabajos derivados así como la fabricación, venta, distribución y uso de productos creados a partir de los archivos de diseño.*

5. ***Redistribución libre:*** La *licencia no debe restringir a un tercero el vender o entregar la documentación del proyecto. No puede ejercerse ningún derecho sobre obras derivadas tampoco.*

6. ***Atribución:*** La *licencia puede requerir documentos derivados y avisos de copyright asociados a los dispositivos. Asimismo debe hacer mención al diseñador.*

7. ***No discriminatoria***: *La licencia no debe discriminar a ningún grupo o persona*

8. ***No discriminación en función de la finalidad perseguida:*** La *licencia no debe de restringir a ningún campo o actividad el uso de la obra.*

9. ***Distribución de la licencia:*** La *licencia se da por distribuida sin necesidad de ir solicitando permisos adicionales.*

10. ***La licencia no debe ser específica de un producto***: *Los derechos de productos derivados hacen extensiva esta licencia.*

11. ***La licencia no debe restringir otro hardware o software***: *No se ponen objeciones a la naturaleza de lo que pueda implementarse a esta tecnología de forma externa o añadida.*

12. ***La licencia debe ser tecnológicamente neutral:*** Ninguna *disposición de la misma debe de basarse en una tecnología específica, parte o componente, material o interfaz para su uso*

Campañas como la lanzada por la EFF, *Defectuosos por defecto* (Defective by Desing)[427], hacen hincapié en la restricción que la fabricación propietaria impone a la hora de tener acceso a nuestro aparatos y a su reparación, lo que no hace más que potenciar la obsolescencia programada de los bienes de consumo. La convocatoria para 2015 de la OSHWA[428] ,ha pretendido finalmente fijar estos parámetros para poder iniciar una comunidad en la que todos los desarrollos actuales puedan confluir.

Otro de los frentes en los que la defensa de la libertad tecnológica está luchando es en el del derecho a reparar, una cuestión que se enfrenta cada vez más a legislaciones restrictivas en cuanto al acceso y modificación de nuestros propios dispositivos. Como veremos en el siguiente capítulo, las intenciones restrictivas han llegado hasta esos extremos y ya existen organizaciones en defensa del derecho a reparar[429].

Uno de los proyectos, enfocados a la robótica que más éxitos han cosechado a lo largo de esta última década es *Arduino*[430]), que ha conseguido que una buena comunidad de desarrolladores empleen su

---

[427] *Defective By Desing*: http://www.defectivebydesign.org

[428] La convocatoria para 2015 de la OSHWA conseguiría ser uno de los eventos mas destacados del sector.: http://2015.oshwa.org

[429] El derecho a reparar, ha tenido un profundo debate en EEUU. Compañías como Apple trataron de elevar a rango legal la imposibilidad de manipular sus dispositivos por parte de los compradores de estos. Finalmente en 2014, se conseguiría reconocer la legalidad de esto y la posibilidad de la reparación por parte de los mismos usuarios: http://www.digitalrighttorepair.org/

[430] Ponencia recogida en TED de David Cuartielles, uno de los cofundadores de Arduino. : https://www.youtube.com/watch?v=yLVrqjPsv64

placa Open Source para diversos proyectos, con especial impacto en la creación de instrumentos musicales o la iniciación en la electrónica de estudiantes. Arduino, nacería en Italia, de la mano de Massimo Banzi y del español David Cuartielles en 2005 con la idea de ofrecer un producto escalable y eficaz de electrónica a bajo costo y es uno de los proyectos con mayor proyección en la actualidad[431].

Otro de los dispositivos que parte de una premisa parecida y que ha tenido un enorme éxito es la *Raspberri Pi*. Lanzada en 2011, se trata de una pequeña placa base de bajo costo (en torno a los 30€), que permite ser empleada en diversos proyectos como si de un ordenador básico se tratara[432]. Su potencialidad y la enorme acogida del producto permitirían que se elaborasen multitud de proyectos para usarla desde servidor de medios y contenidos en el hogar, hasta usos más profesionales como herramienta de trabajo. La expansión del proyeco ha llevado a sucesivas versiones del producto hasta convertirlo en un elemento de referencia para multitud de proyectos. La mas reciente salida de la versión 3 de la placa, junto con una versión reducida con un precio de 5$, ha supuesto un impulso aún mayor al conjunto de desarrollos surgidos en torno a la *Raspberri Pi*.

Por último, La impresión 3D es otro de los terrenos en los existen grandes expectativas de desarrollo. En este campo, la extensión de modelo DIY (Do it Yourself- Hazlo tú mismo) y la difusión tanto de patrones como de modelos de creación están permitiendo un desarrollo paralelo a la gran

---

[431] La web de Arduino, donde se describe el proyecto y se pone a la venta material y se ofrece el software necesario: https://www.arduino.cc/

[432] Web del proyecto Raspberri Pi: https://www.raspberrypi.org

industria de los medios de impresión 3D[433]. Esta carrera no es una cuestión despreciable, dado que el gran terreno que se abre al respecto puede condicionar sectores importantes de la economía futura. En este sentido, el desgaste de la confrontación de las patentes puede jugar en favor de los desarrollos libres, que ya han conseguido algunos éxitos en dicho apartado. La ayuda de integraciones como la de Arduino, están haciendo viables proyectos tecnológicos de impresión 3D domésticos. La cuestión principal del asunto es que se están gestando proyectos de impresoras viables y de código abierto adelantándose a la popularización de la tecnología y su adaptación a producto de consumo. Esta situación, junto a las posibilidades de la fabricación autónoma, puede constituir un elemento con grandes capacidades de sacudir la forma en la que se producen y distribuyen ciertos productos, que podrían imprimirse autónomamente sin control empresarial[434].

Como vemos, uno de los terrenos con más futuro es el de la capacidad de establecer desarrollos tecnológicos no dependientes ni determinados por los grandes de la industria. La posibilidad de que un futuro de estándares abiertos y reconocibles pueda abrirse camino podría ser determinante en un plazo no muy largo.

---

[433] La cantidad de dispositivos 3D con diversos conceptos de hardware libre están modificando una industria antes de su popularizacion: http://faircompanies.com/news/view/impresoras-3d-caseras-hazte-tu-propia-microfactoria-rdi/

[434] *Reprap* es uno de los proyectos de impresora 3D de código abierto de mayor éxito: http://reprap.org/wiki/RepRap/es

3.7 P2P.Legisladores, Propiedad intelectual y piratería. Una colisión de intereses.

Como hemos visto hasta ahora, buena parte de la colisión de intereses que se produce en la red termina por tener una vertiente jurídica y legal. La forma en la que el derecho ha sido empleado por empresas y legisladores para favorecer una serie de intereses y privilegios tiene en la sociedad de la información su expresión más clara[435].Tanto los modelos de negocio basados en la emisión de contenidos en la que el papel del usuario era eminentemente pasivo, como en la difusión de medios culturales, música, cine y literatura, pasando por la prensa escrita, entran en un proceso en el que deben adecuarse a una nueva realidad, en la que los contenidos se popularizan y expanden su accesibilidad. La red ha extendido el acceso a la cultura y muchos de los viejos patrones editoriales no han sabido adaptarse. Como consecuencia de esto, la merma del negocio en crisis, dado que el consumo de medios se ha desplazado a la red, en lugar de trasladarse a una adecuación y actualización se ha recurrido en multitud de ocasiones a forzado legal. Producto de ello, entidades de gestión, como la SGAE española y editoriales de prensa, entre otras, potenciarían que sucesivos gobiernos legislaran de espaldas a una realidad que solo hizo potenciar canales alternativos de distribución. En ocasiones, se trataría incluso de legislar en contra de licencias como la *Creative Commons*, muy usual entre Blogs y medios de Internet, para hacer pasar por un filtro imposible a la nueva competencia.

---

[435] 1. Lessig.L. *Por una Cultura libre. Cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad.* LOM. Santiago, 2005. Edición electrónica: http://www.traficantes.net/libros/por-una-cultura-libre

Los dos resultados más palmarios de esta estrategia derivarían en una crisis de la prensa escrita y la producción, que cada año acentúa su pérdida de lectores, junto con la expansión de alternativas fuera de una legalidad que no dejaba margen a ideas que si tenían éxito. De todo este proceso, se ha derivado que un nuevo dominio en la red comienza a acaparar el mercado del consumo cultural y de medios. De nuevo grandes empresas del entorno digital y otras pioneras, se adueñan de un mercado extenso y creciente aunque distinto al del siglo pasado[436].

En el año 2015 el consumo de música por canales de *streaming* (difusión vía Internet) ya ha superado otras formas de consumo, como la compra en soporte físico. El entorno digital ha forzado los parámetros de la difusión de productos culturales y de medios hacia una adaptación acelerada[437].

Al respecto de la piratería, el propio gobierno de España ha realizado cambios legales sucesivos, todos ellos tomando partido por la restricción de los derechos de autoría y la protección del sistema actual. Para establecer su listado de sitios a cerrar, tomarían los datos de tráfico de *Alexa (*uno de los portales que ofrecen estadísticas más detalladas), de los sitios que comparten contenido con derechos de autor. La nueva Ley de Propiedad Intelectual, ha supuesto la migración y cierre de buena parte de

[436] Lanier, J. *Contra el rebaño digital: Un manifiesto*. Debate. Barcelona. 2011

[437] Informe de la Asociación Promusicae, en el que confirma la tendencia de consumo de música vía streaming, que ya supera a la compra física: Informe sobre música digital 2015: http://www.promusicae.es/anuncios/view/27

las páginas más populares de contenidos digitales[438]. El dato del primer semestre de 2015, tras la entrada en vigor del nuevo cambio legal, hace referencia al cierre de 247 páginas de las 252 que contaban como infractoras de derechos de autor y varias denuncias y detenciones a propietarios de páginas de streaming de contenidos, que se había popularizado al calor de los mejores anchos de banda domésticos de la mano de la extensión de tecnologías como la fibra óptica[439].

Pero, como veremos la economía colaborativa y el P2P (compartir entre pares), es más que el acceso a contenidos restringidos, la vulneración de derechos restrictivos de autoría y su persecución legal. La nueva cultura del acceso, en contraste con la de la propiedad, se abre camino con métodos nuevos, con formas imaginativas de crear redes y una concepción de la propiedad más acorde con la realidad de nuestro tiempo.

El motor económico de la piratería

A lo largo de tres décadas, la existencia de copias no autorizadas de sistemas operativos y software han supuesto una forma de distribución que ha servido para difundir ciertos productos entre sectores que de otro modo o no hubieran disfrutado de estos o habrían directamente hecho uso de otras alternativas libres o más baratas. Así, a pesar de una retórica en favor de la legalidad, ciertas compañías y productos pudieron posicionarse gracias al uso privado de copias no autorizadas de ciertos productos de

---

[438] *Ley de propiedad intelectual* actualizada el 24.11.2014 y puesta en vigor el 1 de enero de 2015. Publicación del el BOE: http://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

[439] El gobierno español se da por satisfecho con la legislación contra la piratería: https://torrentfreak.com/spanish-government-claims-success-in-internet-piracy-fight-150728/

software. El impacto de este uso no ha sido convenientemente estudiado pero si existe un reconocimiento tácito, incluso entre grandes del software como *Microsoft*, como indicamos en capítulos anteriores, que llegaban a reconocer que su modelo *Fremium,* neologismo que hace referencia a una distribución gratuita de un producto comercial normalmente con ciertas limitaciones, ha sido desde siempre la "piratería"[440].

En perspectiva, el posicionamiento de sistemas operativos como el primer *Windows*, o paquetes ofimáticos como Office, que contaban con una competencia muy extendida y eficiente en los terrenos profesionales, no puede explicarse sin la existencia de esas copias que se distribuían en disquetes y los primeros Cds. Cuando un usuario se acomoda al uso de un software normalmente quiere continuarlo en el ámbito profesional. La empresa pudo ser el objetivo prioritario del licenciamiento de software, como bien apuntaban las sucesivas campañas que en nuestro país llevara a cabo por la BSA (Business Software Alliance) y que aún hoy abundan más en vincular seguridad del software legal en sus campañas[441].

Incluso dispositivos de hardware como la primera consola de videojuegos de Sony, la *PlayStation One*, serían grandes beneficiarios del uso de programas fuera del circuito comercial. Esta consola posibilitaba

---

[440] Entrevista al actual CEO de Microsoft, Satya Nadela, donde afirma que su modelo gratuito ha sido la copia pirata: http://www.cnbc.com/id/102101929#

[441] La BSA mantiene delegaciones en la mayor parte de los países desarrollados y es una fuente constante de influencia por parte de los grandes del software: http://ww2.bsa.org/country.aspx?sc_lang=es-ES . Su organigrama y campañas pueden verse en este enlace: http://ww2.bsa.org/country/BSA%20and%20Members.aspx . Una de las ideas más llamativas, tras la búsqueda de la denuncia a empresas por contener software pirata, es la de vincular software ilegal y seguridad. Aprovechando el estallido de incidencias a escala global sobre la ciberseguridad, vinculan ambos casos en sus sucesivos informes: http://globalstudy.bsa.org/2013/cyberthreat.html

mediante la inserción sencilla de un chip y más adelante insertando un cd de arranque preparado al efecto, poder hacer uso de copias de juegos en Cds no originales y disfrutar de estos, lo que permitiría a la compañía posicionarse por encima de grandes fabricantes del momento como *Sega* o *Nintendo*, con modelos más cerrados y por tanto mucho más complejos de copiar. Para Sony, que apenas estaban produciendo juegos por sí misma, el que sus compradores pudieran gozar de un catálogo a precio de Cd copiado suponía la adquisición de una posición privilegiada de ventas y una extensión rápida por un mercado en el que entraron siendo marginales en el sector. De hecho, el propio concepto de la consola con lectora de Cds para juegos les llegaría tras el rechazo de la propuesta de los creadores por parte de la empresa Sega, que lideraba tanto el sector de máquinas recreativas como el de las incipientes consolas de videojuegos con su *Megadrive* y su sistema de cartuchos, mucho más complejos de copiar [442] . La implantación de dichos Chips por parte de pequeños comercios informáticos y usuarios particulares y más adelante la capacidad de permitir esto mismo vía actualización del *firmware* de la máquina (el software base del dispositivo), sería uno de los mayores potenciadores del despegue y hegemonía de los sucesivos modelos de *PlayStation*, hasta su tercera versión. Como vimos en el capítulo precedente, la posición hegemónica hará presentarse a Sony con una estrategia completamente distinta de restricción de la copia y cierre de sus sistemas a cualquier uso no controlado por la compañía[443].

Con estos ejemplos vemos cómo, debajo del debate y el argumentario oficial, diversas compañías han sabido emplear maneras

---

[442] Molist, M. *Hackstory.es. La historia nunca contada del underground hacker en la península ibérica*. 2014. Disponible en formato electrónico en: http://hackstory.es/

[443] Esta web recoge en su wiki todos los métodos conocidos de firmware alternativo para las consolas actuales: http://wololo.net/wiki

extraoficiales de distribución de sus productos para mejorar su posición competitiva, o al menos no han puesto reparos en los beneficios que esta forma de expansión no autorizada les reportaba. La extensión de ciertos productos en mercados donde el acceso a la licencia habría sido una barrear de entrada, ha servido también para tejer una red por parte de las grandes compañías y sus productos. Por otra parte, esta misma extensión informal ha servido de impedimento para el desarrollo de alternativas por parte de comunidades de software libre, que encontraban una competencia muy grande por parte del software copiado[444].

Por otra parte, otra de las grandes dañadas de este modelo extenso de software monopolista ha sido el de los gobiernos o empresas y ámbitos formativos, que han visto como la soberanía tecnológica quedaba en suspenso tras acuerdos globales con las grandes compañías de software para implantar su modelo informático. La soberanía tecnológica queda en este sentido a expensas de multinacionales norteamericanas en su mayor parte y sujeta a un modelo de obsolescencia programada que hace desechar recursos válidos ante el impedimento que las licencias del software necesario para emplear en un dispositivo.

Una sociedad de consumo restringido y la alternativa informal

La democratización al acceso a los contenidos por parte de los usuarios mediante Internet, ha supuesto un revulsivo a los esquemas

[444] Dans, E. *Todo va a cambiar*. Deusto. Madrid. 2010

clásicos de gestión de medios de consumo. Ante las trabas y la falta de adecuación a los tiempos, pronto surgirán alternativas viables, aunque no legales de acceso a los medios. En primer lugar, será, en 1999, Napster, quien iniciará una nueva forma de compartir música. Ante esto, la persecución y el cierre de servidores servirán de acicate para la investigación en nuevas formas de difundir contenidos de forma alternativa a los canales físicos de la época del primer internet. *Audiogalaxy* y sobre todo los archivos *edk*. compartidos mediante servidores repartidos por todo el mundo que gestionaban las ubicaciones reales de los archivos compartidos, iniciaría la revolución P2P. La extensión de *eDonkey* y su clon Emule entre usuarios de las primeras conexiones permanentes permitiría una expansión y una ampliación de contenidos a compartir. La industria del cine y la literatura será la siguiente afectada. Unas programaciones rígidas y a veces erráticas de las series de televisión harían que cada vez más usuarios optaran por la descarga en lugar del visionado en los canales tradicionales. El caso de las series será particular, dado que se tratara de una de las situaciones en las que la difusión de contenidos más se potenciará en las redes. A lo largo de la primar década del siglo XXI, diversas productoras de televisión, especialmente del mercado estadounidense, apostarían por realizar series de mayor calidad que las habituales. Así muchas de estas producciones contarán con presupuestos y medios similares a los de las grandes del cine. Todo ello potenciará en países como España, el consumo de estos productos que años antes apenas tenían impacto, más allá de las más destacadas. Este auge de las series destacará dos contradicciones básicas de los tiempos de la web 2.0: por un lado la falta de traducciones a tiempo y por otro la rigidez de la programación, más sujetas a la disputas de las cadenas que al interés del espectador. Ambos elementos unidos al auge de las líneas ADSL, la aparición de las descargas tipo *torrent* o desde servidores de alojamiento gratuito (que permitían la descarga directa desde sus servidores en tiempos muy breves)

conseguirán una popularización de las descargas consideradas ilegales como no había existido.

Las empresas productoras de contenidos no supieron reaccionar adecuadamente a un consumidor que paulatinamente se había acostumbrado a disponer de los medios de forma independiente de la plataforma. La resistencia y la persecución de la piratería tan solo acentuarán más la difusión y búsqueda de alternativas. En este sentido, ya hemos señalado cómo las propietarias de estas formas de producción de "bienes culturales de consumo", orientadas más al negocio que a la calidad, reconocen que esta forma de resistencia es tan solo una manera temporal de resistir en una forma que irá convirtiéndose en modo residual de su negocio, mientras abren y transforman este en unos nuevos métodos en los que la gratuidad a cambio de inserción publicitaria, o las descargas bajo demanda o mediante canales de previo pago, junto con acuerdos o integración con operadores de comunicación, serán la manera futura de mantener el negocio en estos aspectos. Así, una segunda oleada legislativa en todo occidente, tratara de volver a cerrar las vías abiertas por usuarios de Internet, con el cierre definitivo de la mayor parte de los alojamientos gratuitos a lo largo de 2012 y 2013, con el caso de *Megaupload*[445] como el más destacado y mediático, se volvería a potenciar el resurgir del P2P más descentralizado, con nuevos métodos de compartir archivos *torrent*, mediante enlaces (llamados *magnet*) que no tiene necesidad de ningún servidor ni listado para poder compartirlos o localizarlos. También será el tiempo en el que se potencien los métodos de conexión más segura con la

[445] El cierre de Megaupload creó una gran polémica en su momento, al ser el alojamiento gratuito de mayor éxito y estar a punto de lanzar un sistema de streaming musical alternativo contando con algunos autores de renombre. La orden del FBI con la detención de sus gestores y cierre de sus servidores seguirá un itinerario truculento: http://www.justice.gov/opa/pr/justice-department-charges-leaders-megaupload-widespread-online-copyright-infringement

extensión de servidores privados y VPN (red privada virtual) que permitirá conexiones no transparentes e imposibilitará el rastreo de usuarios que descarguen archivos de Internet, sobre todo tras legislaciones como la inglesa o la francesa, que amenazan con cortar la conexión a Internet de los usuarios cuyos ISP (proveedores de servicio de Internet) señalen como descargadores de contenido con derechos de autor.

No es tarea del presente trabajo describir los métodos más recientes y la forma en la que usuarios, gobiernos e ISP, han mantenido una dialéctica en la que las descargas, de un modo u otro han permanecido. Señalaremos que incluso en los momentos de mayores cierres, como los sucesivos arrestos e incautaciones de datos de *Pirate Bay*, el mayor portal de archivos *torrents* existente, las variaciones de consumos y descargas apenas han sufrido mermas globales, producto de la búsqueda y acomodación de los usuarios de nuevos métodos y lugares[446]. Lo cierto, es que todos los años transcurridos desde que la web 2.0 comenzara su andadura y la concreción de modelos de negocio de medio coherente con esta ha permitido la gestación de una cultura alternativa de lo compartido. Con ello, han arraigado esquemas y comunidades en las que compartir diversos medios culturales es visto como una cuestión fundamental de la existencia digital. La presión de los medios y la desproporción de la acusación de piratería a la copia de medios han supuesto una quiebra en la identidad con muchos artistas, que son considerados serviles de los grandes poderes del medio, empresas, sociedades de gestión de derechos

[446] El documental TPB AFK: The Pirate Bay Away From Keyboard, creado mediante financiación colectiva (crowfounding) es uno de los documentos más esclarecedores de cómo se organiza un servidor gratuito de servicio de archivos torrent para la descarga. El caso de *The Pirate Bay* ha sido paradigmático del resto de grupos de usuarios dado que es la base de datos más grande que existe hoy en día de este tipo de archivos y los sucesivos y recurrentes cierres no han conseguido frenar la reaparición de sus servidores en diferentes lugares. El documental pude verse en: https://www.youtube.com/watch?v=eTOKXCEwo_8

y gobiernos plegados a sus intereses. Si a todo esto unimos una cada vez mayor escasez de márgenes personales para disponer de dinero que pueda ser destinado al consumo cultural, producto de un empobrecimiento colectivo del trabajador medio, hecho potenciado aún más tras la crisis económica, no es de extrañar el auge de medios considerados ilegales de acceso a la cultura[447]. La incorporación al medio digital de cada vez más medios culturales, desde el comienzo musical y cinematográfico, hasta el auge del eBook más reciente, ha potenciado aún más estos cauces de consumo alternativos. El ascenso de economías informales entre poblaciones en proceso de empobrecimiento no es algo nuevo en el análisis social. Sin embargo, en este caso estamos tratando de la posibilitad de acceso a bienes culturales digitales, que rompen barreras que habían existido a lo largo de toda la historia de la humanidad. Nunca antes, la práctica totalidad de una población había dispuesto de medios para acceder a cualquier bien cultural sin más precio que el acceso a la red y la interfaz tecnológica. La popularización del Smartphone y otros dispositivos de reproducción y acceso han supuesto una ventana global a la cultura sin distinción de clase. En este contexto, la consideración legal del acceso es totalmente secundaria y depende más de las estrategias de negocio y la adecuación del marco legal de quienes producen los medios masivos que de quienes los consumirán, en busca siempre el cauce más simple y en función a sus posibilidades. Así, aunque con rangos de calidad en algunos casos inferiores y una experiencia final diferente, la posibilidad de llegar a un público global ha superado cualquier otra barrera. El error de muchos medios ha sido confundir obstáculo con límite[448].

---

[447] Rifkin, J. *El fin del trabajo. Nuevas tecnologías contra puestos de trabajo: El nacimiento de una nueva era.* Paidós. Barcelona. 2004

[448] VVAA. *Manifiesto Cluerain* http://www.cluetrain.com/ Las tesis en castellano están disponibles en: http://tremendo.com/cluetrain/ . 1999.

A pesar del fuerte empuje y resistencia del modelo de descarga y consumo alternativo a los cauces legales de medios digitales, la segunda década del presente siglo ha comenzado a dejar ver alternativas viables de consumo de contenidos con derechos de autor respetando la legalidad establecida. Uno de los pioneros en este sentido ería la tienda de Apple integrada en iTunes (el medio de sincronización de dispositivos móviles de Apple). Con un precio unitario de canción de un dólar estadounidense, el usuario de las diversas generaciones de iPod e iPhone, pudo disfrutar de estas en sus dispositivos móviles. Desde la aparición del primer iPhone, en 2007, la posibilidad de empleo como reproductor de medios será una función básica, a la altura del de uso como teléfono y cada vez en más medida como ventana a la red. Como ya hemos comentado, la conversión de todos los medios de consumo digital hacia la movilidad y la convergencia de todas las plataformas hacia una función polivalente, en la que el usuario quiere disponer de sus contenidos en cualquier dispositivo que emplee en cada momento del día, es la piedra de toque de la tecnología de consumo del presente siglo. La adaptación a esa necesidad se ha convertido en el *leitmotiv* de cualquier presentación de nuevos productos en las sucesivas citas tecnológicas que salpican el calendario, como el *Barcelona Movile Congress* o el *CES* de las Vegas, por dos de los más mediáticos[449].

El caso de *Spotify* es ejemplo de ese nuevo modelo de negocio, del que ya hemos explicado su funcionamiento anteriormente. En esencia, se trata de un portal de *streaming*, con aplicaciones para diversas plataformas, especialmente en dispositivos móviles que nos permite oír

[449] Echeverría, J.: *Los Señores del aire: Telépolis y el Tercer Entorno*. Barcelona (Destino) 1999

cualquier álbum de cualquier artista de su amplio catálogo. Incluso en su versión gratuita, que inserta cortes publicitarios y tiene limitaciones de calidad de sonido, nos abre ya grandes posibilidades que dejan sin mucho sentido buena parte de los escenarios de descarga de música. Las versiones para teléfono o sin restricción son de pago, y grandes multinacionales de la producción musical de consumo, como *Sony Bmg*, pronto han prestado su fondo discográfico para esta aplicación. En un principio, esta compañía sueca vería como su modelo de negocio entraba en disputa con la legislación de derechos de autor en EEUU, hasta los extremos de tener que sufrir una restricción temporal de sus servicios para clientes de este país. Como ya explicamos en el capítulo dedicado a la expansión de los servicios en línea, pronto todas las grandes de Internet pasarán a ofrecer su producto musical en streaming. Para entender la tensión entre la restricción de modelos de negocios y la irrupción en estos hay que comprender cómo se han concentrado los medios de producción que acaparan la mayor parte del valor comercial. El cambio de paradigma, ya definitivo e imparable, ha impulsado de este modo a la conversión digital y definitiva de catálogos en pos de un negocio que busca conquistar tanto la movilidad como el centro del salón doméstico, en el que la televisión convencional ha perdido su posición dominante[450].

El terreno de los medios de comunicación masiva no dejará pasar esta oportunidad y junto con la convivencia de formas y medios tradicionales, televisiones generalistas y difusión cultural con mecanismos tradicionales como la impresión de libros y discos, podemos ver cómo se buscan nuevas formas de negocio. Teniendo en cuenta que la mayor parte

---

450

16. VVAA. *Cultura digital y movimientos sociales*. Catarata. Madrid. 2008

de los medios son privadas la oferta mejorada que busca sustituir el espectáculo pasivo de la radio y televisión tradicional pasa por una oferta digital de pago. Heredera de las plataformas digitales por satélite, la actual oferta de televisión, comienza aunar la parrilla diversa de programas junto con servicios más similares al streaming, como grabado de programas mediante dispositivos de reproducción mixtos o canales "a la carta" que pueden ser vistos como si de un portal de video de internet se tratara. La existencia de plataformas directamente dedicadas al streaming capaces de llegar al televisor familiar, como Hulu o Netflix, en EEUU son una amenaza al monopolio de la producción y la oferta televisiva y por ello, la carrera ya no es por ofrecer una alternativa a la piratería de contenidos sino al método de ofrecerlos, una vez que el usuario tiene acceso a una red con ancho de banda suficiente. De nuevo, el cierre a la posibilidad de implantar el modelo de televisión en *streaming*, por los precios de la gestión de derechos, potenciaría el auge de plataformas de *streaming* mediante servidores privados o vía P2P, como *Popcorntime*, cuyos "clones" (copias o servicios similares) se multiplican en la actualidad[451]. Este último caso es especialmente significativo al suponer una alternativa simple, eficaz e incapaz de ser cerrada por el legislador de turno a los sistemas de *streaming* que en países como España no han llegado a tiempo debido a trabas legales.

De cualquier modo, vemos cómo las grandes compañías propietarias de la mayor parte de los derechos de autor de la producción cultural, mantienen, a pesar de la clara consciencia de que el modelo de

[451] El caso de *Popcorntime* y sus clones http://popcorn-time.se/ y https://popcorntime.io/ merece especial mención, al tratarse de un sistema multidisposivo que aprovecha las redes entre iguales para sin conocimientos poder disfrutar de un catálogo ingente de películas y series. La simplificación de la manera de acceder a este y la incapacidad del legislador de turno de cerrarlo (está distribuido) lo sitúan en cuanto a calidad y capacidad a la altura de alternativas comerciales.

negocio conocido hasta ahora tiene una trayectoria más que limitada, un férreo control mediante sociedades de gestión de derechos de autor como la RIAA estadounidense o la SGAE española, al servicio de la concentración de medios comerciales. Como hemos señalado, el provecho legal y la ventajosa posición de cara a unos medios cada vez más concentrados han posibilitado la difusión de una imagen distorsionada de la realidad de un negocio cada vez más orientado al beneficio económico y por tanto cada vez más distante de la producción artística. Siete grandes corporaciones (AOL-Time Warner, Disney, Sony, News Corporation, Viacon y Bertelsmann), controlan la práctica totalidad de la producción mundial audiovisual, tanto en los medios como en los contenidos[452]. El acuerdo con los ISP mayoritarios de cada país, les han permitido la integración de servicios y el mantenimiento de cuotas de control.

En este sentido, podemos ver cómo las programaciones de diversos medios convergen en unas metodologías similares para, finalmente, resultar apenas distinguibles, sería un ejercicio interesante para llevarnos a reflexionar si la exclusiva búsqueda de negocio y la mercantilización cada vez más extensa consiguen establecer algún nexo con la calidad. En lo que respecta a nuestro país, el espejismo de la TDT, que se prometía como la llegada de una auténtica variedad y ampliación de contenidos, ha quedado en manos de dos grandes grupos mediáticos, *Atresmedia* y *Mediaset*, que se reparten la práctica totalidad de la parrilla televisiva con programaciones similares y concurrentes[453]. Algo que ya ocurriría en la anterior oleada de plataformas de televisión digital por satélite, que finalmente terminarían convergiendo y en la actualidad se encuentran en proceso de conversión hacia la tecnología digital aprovechando la

---

[452] VVAA. *Cultura digital y movimientos sociales*. Catarata. Madrid. 2008

[453] Castells,M. *Innovación, libertad y poder en la era de la información*. Artículo en Sociedad Mediatizada. Gedisa. Barcelona.2007

infraestructura de cable y las ofertas convergentes de las proveedoras de Internet. El camino hacia el envejecimiento de las audiencias de la televisión convencional no se ha paliado con el fenómeno del *reality* que se extiende a lo largo de toda la parrilla y la tertulia autorreferente y banal. La realidad formateada de las televisiones generalistas carente de un contenido vive un proceso imparable de abandono por parte de las generaciones más jóvenes[454].

La pérdida de este referente general junto con el monopolio de la información por parte de los medios escritos ha sido uno de los acicates de una legislación tan restrictiva como la que aprobara la "Tasa Google", dentro del articulado de la antes mencionada Ley de Propiedad intelectual. Así el denominado Canon AEDE (Asociación de Editores de Diarios Españoles) , término acuñado por la *Coalición Pro Internet*, que confronta con la agrupación de medios promotores de la entrada en vigor de esta Ley, trataba de hacer pagar a los portales que suministren enlaces a noticias de otros medios. Algo no solo contrario a la naturaleza de la red sino perjudicial, ya que la profusión de enlaces mejora el posicionamiento de las webs y por tanto mejora su visibilidad de forma inmediata y gratuita[455]. La reacción de Google ante la entrada en vigor de esta ley que penaliza el enlace sería la de retirar su portal de noticias Google News el mismo día 1 de enero. La penalización a los medios de AEDE en su buscador sería inmediata, con la subsiguiente merma en ingresos publicitarios de Internet y la búsqueda de mejorar sus cuentas a cuenta del buscador un intento vano. Mientras tanto *agregadores* como *Menéame*, se

---

[454] 21. VV.AA. *Sociedad Mediatizada*. Gedisa. Barcelona.2007

[455] La Coalición Pro Internet Agrupa a buena parte de las asociaciones de activistas de Internet españoles http://coalicionprointernet.com. En la siguiente página explican su postura y oposición al establecimiento de una ley en favor de los grandes medios editoriales: http://coalicionprointernet.com/?page_id=567

ven empujados a salir de España para mantener el medio. Todo este movimiento de influencia de medios hasta hace poco hegemónicos en la gestión de noticias se debe tanto a la necesidad de doble vía de mantener el *statu quo* mediático y su relación (cuando no total identidad) con el poder, como por la mala gestión de la edición digital. Efectivamente, como afirma Lorenzo Vilches, la pereza de estos medios ante su posición privilegiada precedente, les llevaría incluso a plantear plataformas de pago para el acceso a sus contenidos, mientras las alternativas mucho más horizontales y participativas se estaban gestando[456]. Actualmente, el enlace y la *socialidad* de un medio pueden darle más credibilidad que unas líneas editoriales muy rígidamente trazadas. La crisis de los medios escritos tiene mucho de actualización al mercado digital, donde otros medios más identificados con el público que los consume avanzan, pero tampoco es ajena a la rigidez monocolor de sus líneas editoriales y su relación con los gobiernos de turno[457].

Mientras se hace extensivo este modelo de cultura restringida y dirigida, nuevos actores irrumpen en la producción. La autoedición de libros, con el ascenso del *eBook*, es uno de los fenómenos más destacados de este proceso. Una de las compañías que mejor han sacado provecho de esto ha sido *Amazon* que vende varios dispositivos de lectura de medios a precios muy competitivos enfocados al consumo de los productos que ofrecen en su tienda. La tienda de libros *Kindle* de *Amazon* cuenta en nuestros días con un catálogo de 142.081títulos en castellano y un sistema de venta directa a dispositivos móviles y un esquema de comisiones del 30% a los autores que autoeditan que le ha permitido hacerse como la tienda hegemónica en el mercado de libro

[456] VV.AA. Sociedad Mediatizada. Gedisa. Barcelona.2007

[457] VVAA. Cultura Libre Digital. Icaria. Barcelona. 2012

electrónico[458]. Las estructura del negocio editorial, a pesar de los años transcurridos desde que los inicios delo primeros libros electrónicos vería como se alzaba un gigante del medio digital mientras el mercado editorial clásico se enfrentaba a un paulatino descenso es sus cuotas de mercado.

Por otra parte, cadenas como HBO, que mantiene cierta independencia de su matriz Time-Warner e incluso más recientemente de *streaming*, como *Netflix*, se han lanzado a la creación de uno de los productos audiovisuales que más consumidores reciben, las series. Como hemos señalado, el auge de este tipo de productos ha venido de la mano de las series televisivas que se han convertido en el patrón de calidad de las cadenas. Así de un producto menor casi de relleno de horarios, las series son ahora el motor de muchas cadenas que cuentan con producciones millonarias inspiradas a su vez en fenómenos editoriales en muchos casos. La serie televisiva, ha trasladado en parte las formas de la novela para establecer una narrativa larga en la que poder desarrollar tramas y personajes sin las restricciones del cine convencional. Así, se ha permitido que historias imposibles en el cine puedan ser narradas con tiempos distintos, mediante capítulos. Pero los tiempos de las series son otros y la forma de consumo ha cambiado. Por ello, las cadenas avanzan en modos de emisión diferentes, entre los que destacan el antes señalado del streaming. El público no está dispuesto a modificar sus tiempos a los de emisión de una cadena. Un nuevo tipo de consumo más activo busca

[458] El sistema y catálogo de la tienda de Amazon permite la gestión y compra sencilla de libros y su importación inmediata en el dispositivo de lectura, siempre sincronizado. Incluso algunos de sus lectores de libros electrónicos cuentan con conexión de datos exclusiva para la sincronización y descarga de los libros adquiridos: http://www.amazon.es/comprar-libros-espa%C3%B1ol/b/ref=topnav_storetab_b?ie=UTF8&node=599364031

gestionar su momento de visionado y por tanto son los que ofrecen el medio los que se adaptan para no ser fagocitados por las descargas.

Otros colectivos de creadores partirán de una premisa no comercial o al menos no obligatoriamente orientada a la venta para dar a conocer su obra. Entre los más destacados, artistas plásticos como los que se agrupan en *Devianart*, fotógrafos como *Pixabay* o músicos en medios como *Jamendo* ofrecerán su obra con licencias Creative Commons, la mayor parte de ellas permitiendo el uso no comercial de esta [459]. Las características de muchos de estos portales se asemejaran a las dinámicas ya conocidas por usuarios de redes de descarga de medios con derechos e incluso se permite acceso mediante distintos soportes[460]. Así los nuevos creadores, nacidos manejando la red, se integran en está cambiando los tradicionales roles de la producción y la edición. La nueva forma de gestión cultural surgida tanto de movimientos politizados en favor de las licencias *Creative Commons* y el *Copy Left* en general, como por creadores independientes no suscritos a la dinámica del mercado tradicional de la cultura, se abre camino a través precisamente de la red y las nuevas formas de comunicación horizontal[461].

---

[459] VVAA. CopyLeft. Manual de uso. Traficantes de sueños. Madrid. 2006. Recurso con licencia *Creative Commons* también disponible en: http://www.articaonline.com/wp-content/uploads/2011/07/Copyleft-Manual-de-uso.pdf

[460] Lessig.L Remix. Cultura de la remezcla y derechos de autor en el entorno digital. Icaria. Barcelona 2011

[461] Lessig.L. El código 2.0. Traficantes de sueños (licencia Creative Commons), Madrid. 2009.

Toda la cultura alternativa al circuito comercial de las grandes productoras ha vivido a lo largo de estos años un proceso de toma de conciencia y politización debido precisamente a la reacción contraria de los legisladores en favor de los poseedores del mercado establecido[462]. En este sentido, los defensores de las licencias *Creative Commons* en general han tenido un itinerario similar al vivido por el colectivo en torno a las licencias GNU[463]. La falta de un sistema claro de registro de obras digitales y el reconocimiento no completamente formal de otras formas de registro de obras digitales más allá del registro clásico, como hacen bases de datos como *Safe Creative*, enfocada a la creación digital[464].

El DRM y la neutralidad de la red

El DRM (Digital Rights managament- Administrador de Derechos Digitales) ha sido uno de los últimos intentos de controlar la difusión de contenidos por medio de la red. La idea fundamental de este sistema es la de fijar una serie de parámetros que obliguen a la identificación del medio respecto a su consumidor, para que mediante un estándar de cotejo pueda confirmarse que ha pagado y por tanto dispone de permiso para su uso. El debate sobre la inclusión de este sistema llegaría a crear un conflicto entre los desarrolladores de navegadores como Firefox, entre los que se oponían

---

462 VVAA. *CopyLeft. Manual de uso*. Traficantes de sueños. Madrid. 2006. Recurso con licencia *Creative Commons* también disponible en: http://www.articaonline.com/wp-content/uploads/2011/07/Copyleft-Manual-de-uso.pdf

463 Fundación CopyLeft. Entidad española dedicada a la difusión de licencias tipo CopyLeft entre artistas y creadores: http://fundacioncopyleft.org/

464 Safe Creative: La primera entidad de registro de obras de propiaedad intelectual en Internet: http://www.safecreative.org . El registro de todos los tipos de obras está disponible en: https://www.safecreative.org/?wicket:interface=:6:::

a incorporar dicha capacidad y los que solo hablaban de compatibilidad con entornos que iban a implantarse. En concreto la polémica vendría por permitir el sistema EME (*Encrypted Media Extensions*) de la empresa Adobe, para restringir mediante cifrado contenidos de video y sonido. Una de las peores consecuencias del DRM en los navegadores es que dejan una puerta abierta a la gestión de la conexión de los usuarios por parte de las gestoras de estos derechos, que conectan con sus bases de datos para las pertinentes comprobaciones y por tanto pueden comprometer la intimidad de los usuarios[465].

Lawrence Lessing, hace distinción entre cierta tipología de propiedad que protege los derechos frente a otra que ejerce una actitud parasitaria respecto a estos. Es decir, el respeto a los derechos de autoría tiene formas suficientes con las licencias *Creative Commons*, que no da lugar a negocio con la obra si no se cuenta con el autor, pero impide que elementos ajenos al creador se conviertan en rentistas del derecho mercadeado con este[466]. La propiedad intelectual restrictiva supone en nuestro tiempo un obstáculo al desarrollo entre los que no tienen recursos para acceder a través de esta. Como afirma Castells, se trata de un tema eminentemente político en el que los pobres del mundo, los creadores y los innovadores deben tener como objetivo común la reforma de la propiedad intelectual tal y como hoy en día es entendida[467].

---

[465] El revuelo en la comunidad de apoyo a Mozilla Firefox cuando implementó en su versión 38 el famoso DRM es recogido por los activistas de EFF: https://www.eff.org/deeplinks/2014/05/mozilla-and-drm

[466] Lessig.L. *Por una Cultura libre. Cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad.* LOM. Santiago, 2005. Edición electrónica: http://www.traficantes.net/libros/por-una-cultura-libre

[467] Castells,M. *Innovación, libertad y poder en la era de la información*. Artículo en Sociedad Mediatizada. Gedisa. Barcelona.2007

Al igual que con las patentes de software, otro terreno de gran disputa en la actualidad es el de la neutralidad en la red. Mientras ciertas empresas quieren ofrecer una red a doble velocidad, priorizando servicios propios o producto de acuerdos, como las un WhatsApp o un Facebook sin cargos de tarifas de datos a ciertas operadoras de telefonía móvil, o la priorización de ciertos motores de búsqueda, cierran el camino a cualquier intento de competencia, lastrado por penalizaciones de usabilidad y velocidades de conexión con cargos adicionales. Actualmente el tema sigue en pleno debate y hasta lo que han llegado ciertas operadoras es a ofrecer tarjetas de datos que no cuentan los accesos a WhatsApp o Facebook o Skype, dependiendo de la empresa que las promueve[468]. Aunque en EEUU se cerraría el caso recientemente y el debate en la propia UE, la idea sigue apareciendo de forma recurrente[469]. La sombra permanece dado que aunque la UE aprobó a finales de 2014 un documento acerca de la neutralidad de la red, defendiendo la igualdad de acceso, por otra parte mantiene una postura contraria con líderes como Ángela Merkel, que se ha posicionado a favor de potenciar ciertos servicios de Internet respecto al resto del tráfico. En este sentido, la capacidad lobista de los proveedores de Internet plantea de forma recurrente ciertos debates. No es un caso aislado, como hemos visto con el TTP a lo largo de 2015, tras descartar ACTA, en los temas relativos a los derechos de autor. Este enfoque, en el que de un modo u otro convergen bastantes

[468] . Sobre las tarjetas de prepago con acceso whatsim, existe una gran polémica dado que son el exponente y el experimento previo de una red que margina usos. Extender este tipo de tarjetas de consumo dirigido entre el público más joven trata de encauzarlos por una serie de servicios que solo rinden cuentas a las grandes empresas es la puerta de entrada a una red no neutral. Una de las más señaladas en los medios ha sido la que ofrece exclusiva de uso con WhatsApp si cargos: http://www.whatsim.com/index.html

[469] . EDRI elaboraría un documento sobre las decisiones del Consejo europeo y el eurparlamento acerca de la neutralidad en la red y su debate actual: https://edri.org/files/NN_analysis_20150715.pdf

compañías de las grandes de Internet y el sector de las telecomunicaciones, vuelve a contar con el factor de la influencia en los miembros de los gobiernos con capacidad de decisión, entre los que se potencia un debate, creado expresamente en beneficio de empresas privadas[470].

El debate en torno a los derechos de autor ha llegado a extremos en los que se han planteado legislaciones incluso sobre el llamado derecho al panorama. Esta limitación hace referencia a la propiedad limitada de ciertos paisajes por parte de los propietarios del mismo. La cuestión, ya chocante en una sociedad en la que la fotografía digital y la de viaje son cada vez más populares cuando conocemos restricciones como las que tienen monumentos como la torre Eiffel. Como es de suponer, el monumento tiene edad suficiente como para no tener restricciones por sí mismo. Sin embargo, el autor de la iluminación nocturna de esta, se atribuye unos derechos de autoría que afectan a las fotografías nocturnas de este e impiden la venta y uso sin permisos de las fotografías nocturnas que se tomen. Sírvanos el ejemplo como muestra de los grados de absurdo a los que pueden llegar las atribuciones de derechos de autor. La curiosa disposición de ciertas leyes de propiedad intelectual, al calor de la Directiva 2001/29/CE del Parlamento Europeo, que permite a las diversas naciones restringir en sus territorios la libertad de panorama, fue llevada a debate en el seno del parlamento europeo el pasado 9 de julio de 2015, que finalmente siguió dejando en manos de cada país la gestión del

[470] Sobre la neutralidad en la red La Quiadrature du net, tiene extenso material sobre campañas legislativas de la UE: http://www.laquadrature.net/en/Net_neutrality

derecho aunque no permitiendo la aprobación de la extensión de esta restricción al ámbito europeo[471].

P2P y economía colaborativa

Como señalábamos, compartir entre pares no solo es un método de hacer llegar contenidos y transmitirlos de forma social, tengan o no restricciones por derechos de autor sino que se está convirtiendo en una nueva forma de establecer cauces de establecimiento de principios económicos horizontales[472]. Si los negocios, con los modelos B2B (de negocio a negocio) y B2C (de negocio directo al consumidor) han conseguido aprovecharse del trato directo de la red para llegar directamente, los propios consumidores, tomando posesión de su papel esencial en cualquier economía, también pueden establecer cauces comunes de comunicación y venta[473]. El auge de la red a permitirá saltarse cauces de intermediación para legar directamente del producto al consumidor. El siguiente paso es crear redes de economía solidaria tal y como la proponen comunidades como *Ouishare*[474], mediante la creación de un entramado de iguales capaces de tomar una actitud activa en el consumo y por tanto ser parte activa del proceso. Ejemplos como *La Colmena Dice Si*, son un referente en cuanto al apoyo de la producción

---

[471] Directiva europea que permite a las naciones restringir la libertad de panorama. http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32001L0029

[472] Dans, E. *Todo va a cambiar*. Deusto. Madrid. 2010

[473] Rifkin, J. *El fin del trabajo. Nuevas tecnologías contra puestos de trabajo: El nacimiento de una nueva era.* Paidós. Barcelona. 2004

[474] La comunidad de economía colaborativa OUISHARE pretende establecer unos parámetros de horizontalidad en las relaciones económicas entre personas: http://www.ouishare.net/en. Noticias en castellano en: http://magazine.ouishare.net/es

local y la ejecución de redes de venta y consumo directo de productos alimenticios [475] . En esencia se trata de recuperar mercados locales sostenibles en un modelo que confronta con las grandes superficies y sus formas de producción y transporte.

Casos como *Uber*, o *Airbnb*, están empañados de polémica al establecer competencia directa con los sectores del taxi y el hotelero respectivamente. Efectivamente, la precarización, puede haber encontrado su reverso en nuevas formas de establecer el negocio. Si por ejemplo, el sector turístico, ha sacado partido de los años de crisis para restringir sus costos laborales mientras ampliaba resultados, no es de extrañar que el modelo se extienda a la posesión individual y la forma de sacarle partido. En este sentido, la puesta a disposición de vehículos particulares o viviendas, anunciándose en plataformas que atajan todo tipo de intermediarios debería ponerse en relación a la cultura de la precariedad que se ha ido extendiendo, especialmente entre las capas más jóvenes de las sociedades urbanas occidentales [476] . El aumento del Freelance, autónomos ante la falta de contrataciones reales estables junto con una idea menos fijada en la propiedad, tal y como la entendían generaciones anteriores y más centradas en el uso ha potenciado conceptos. Así otros medios de puesta en común como *BlablaCar* o de venta directa entre particulares como *Wallapop*, parten del mismo concepto de libertad.

---

[475] La colmena dice sí, es un proyecto que aúna productores y consumidores en marcados locales que comenzara en Francia y ya comienza a extenderse por España: https://laruchequiditoui.fr/es

[476] Rifkin, J. *El fin del trabajo. Nuevas tecnologías contra puestos de trabajo: El nacimiento de una nueva era.* Paidós. Barcelona. 2004

Un movimiento que está alcanzando gran notoriedad en EEUU es el de los colectivos que reivindican el derecho a reparar, una reivindicación respecto a la libertad tecnológica y contra la obsolescencia programada[477]. El colectivo ha planteado sucesivas campañas en las que hacía hincapié en el modelo productivo conscientemente defectuoso de la producción de bienes en occidente, como *Defective By Desing* (diseñado defectuoso)[478]. Especial relevancia tendría el asunto cuando Apple tratara de negar la posibilidad de acceder a los dispositivos de su marca si no era en tiendas oficiales. Un largo itinerario judicial terminaría por reconocer el derecho a la reparación de todos los dispositivos propiedad del ciudadano y su pertinente manipulación para uso personal en 2014, con la pertinente reforma de la DMA (ley de derechos de autor estadounidense)[479]. La parte más interesante de este movimiento es su colaboración a través de la red para recrear manuales de reparación de productos que no los ofrecen al público. En páginas como *Ifixit* podemos encontrar multitud de guías detalladas de cómo reparar productos de las marcas más conocidas con tutoriales e incluso vídeos ordenados por grados de dificultad[480].

La tendencia a las economías cooperativas es el paso consecuente a la extensión de las redes sociales y las formas de aprovechar los medios

---

[477] El derecho a reparar, ha tenido un profundo debate en EEUU, sobre todo frente a la imposibilidad inicial de acceder no solo al interior de los dispositivos sino a que se considere legal dicho acto: http://www.digitalrighttorepair.org/

[478] Defective BY Desing: http://www.defectivebydesign.org

[479] http://www.fixthedmca.org/ Campaña para delimitar la ley DMA estadounidense sobre patentes que impide la publicación de manuales de reparación.

[480] El sitio Ifixit, es toda una referencia a la hora de encotrar manualles y métodos de reparación de cada vez mas dispositivos. https://www.ifixit.com/ . Con la inclusión de una aplicación móvil, la comunidad ha conseguido una gran expansión entre usuarios que la toman como una referencia previa a los servicios oficiales, que en muchas ocasiones responden a los principios de la obsolesciencia programada no llegando a reperar según que elementos.

y formas de comunicación de la nueva era por parte de los usuarios de la red. Por tanto, las formas de colaboración social y la extensión de comunidades y medios colaborativos se encuentran en proceso de expansión. Si en primer lugar las redes fueron sitio para pioneros digitales y grandes empresas, con la extensión y popularización de las comunicaciones, es el conjunto de la sociedad la que apunta a la red como forma básica de encontrar respuesta a cada vez más necesidades. Así la extensión del consumo social y las nuevas formas de colaboración apenas han comenzado a la hora de redactar este trabajo; por ello no podemos más que establecer una pequeña alusión sobre las perspectivas que este terreno abre. Un camino en el que la sorpresa que ha acompañado a muchos otros sectores tradicionales podría extenderse en el terreno del autoconsumo y el consumo responsable. Sería un paso posible dado que la red ya ha revolucionado otros sectores que no siempre han quedado conducidos por la gran empresa.

Sobre Creative Commons

Creative Commons es el modelo de licencias tipo CopyLeft más extendido en la actualidad entre creadores. Es muy empleado en blogs y portales de noticias así como entre creadores audiovisuales.

http://es.creativecommons.org/blog/licencias/

Existen seis modelos de licencias a disposición de autores según más les convenga:

Reconocimiento: Se permite cualquier explotación de la obra, incluyendo una finalidad comercial, así como la creación de obras derivadas, la distribución de las cuales también está permitida sin ninguna restricción.

Reconocimiento - NoComercial (by-nc): Se permite la generación de obras derivadas siempre que no se haga un uso comercial. Tampoco se puede utilizar la obra original con finalidades comerciales.

Reconocimiento - NoComercial - Compartir Igual (by-nc-sa): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

Reconocimiento - NoComercial - SinObraDerivada (by-nc-nd): No se permite un uso comercial de la obra original ni la generación de obras derivadas.

Reconocimiento - Compartir Igual (by-si): Se permite el uso comercial de la obra y de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

Reconocimiento - SinObraDerivada (by-nc): Se permite el uso comercial de la obra pero no la generación de obras derivadas.

IV: Internet como instrumento de conflicto y democracia

4.1 Una sociedad auditada: Bases de datos y vigilancia mundial

Como ya vimos en el bloque primero, en el capítulo dedicado a *Redes espías y satélites*, la red mundial y otros avances técnicos, pronto estarían a disposición de fines de vigilancia y espionaje, en primer lugar de gobiernos, especialmente el norteamericano, para pasar paulatinamente a instituciones privadas y sobre todo las empresas del sector, que comenzarán a atesorar datos personales de millones de usuarios so pretexto de "usabilidad" de motores de búsqueda, persistencia de *cookies* (elementos identificativos que son enviados a ciertas páginas Web al acceder a estas) o recogida de datos de carácter personal para disponer de ciertos servicios. Analizando los datos que vamos conociendo, de forma indirecta en muchas ocasiones, podemos establecer dos líneas convergentes en cuanto a la vigilancia y control de los datos, por un lado los gobiernos, su policía y agencias de vigilancia y espionaje y por el otro las grandes corporaciones dedicadas a negocios en red y que cada vez reconocen como más útil la adquisición de datos de carácter personal, tanto para uso propio como para su venta a otras entidades.

La primera de estas tendencias, ya expuesta desde sus orígenes, como señaláramos, al tratar sobre la red de escuchas global *Echelon*, o el programa TIA (Total Information Awareness- Vigilancia Informática Total), se vería impulsada en mayor medida aún tras los atentados del 11-S en EEUU, excusa perfecta para la promulgación de la *Patriot Act*, que permite poner en suspenso derechos individuales so excusa de la seguridad nacional y la lucha contra el terrorismo, que parece incluir activistas de derechos sociales e incluso a organizaciones como *Greenpeace*. Un avance en este sentido sería la *Homeland Security Act*, de 2003, que pretendía la recogida global de datos biométricos completos de todos los

ciudadanos norteamericanos y cuantos extranjeros fuese capaz por múltiples vías, incluyendo el acceso a ficheros de compañías privadas, por otro lado siempre abiertas a una colaboración que respalde su actividad, y tratando de identificarlos en todo momento mediante la integración de sistemas de identificación a distancia y videovigilancia[481]. Ante lo costoso del proyecto, el congreso retiraría su apoyo económico, aunque otras agencias, como el FBI, plantean crear un fichero parecido, en el proyecto denominado NGI (Next Generation Identification), que recopilaría informaciones antropométricas de todos los individuos posibles para su reconocimiento por todos los medios de vigilancia disponibles, con especial hincapié en la videovigilancia continua de zonas públicas. En esa misma dirección, apunta el CITeR (Center of Identification Technology Research), que trata de avanzar en escáneres capaces de dicho reconocimiento facial instantáneo a 200 metros y del iris a tres metros. Parecidas investigaciones están llevándose a cabo, so excusa del terrorismo y la seguridad, por parte de diferentes gobiernos europeos.

En el ámbito comercial, también diversas aplicaciones como el *Eye Movement Recorder*[482], pretende un control de los hábitos de consumo de los clientes de supermercados para poder "guiar" las pautas con las que se dirigen a la hora de comprar. La puesta a disposición de dichas herramientas de control a los organismos oficialmente dedicados a la "seguridad" será la excusa perfecta para la implantación progresiva de métodos cada vez más refinados de control y dirección del consumo por parte de las empresas. Las propias directrices de la *Homeland security*,

---

[481] Preuss-Laussionotte, S. *La democracia ante los riesgos de la mundialización de las bases de datos.* En El estado del mundo 2009. Akal, Barcelona 2008.

[482] Ramonet, I. *Pensamiento único y nuevos amos del mundo*. Icaria. Barcelona. 2008

suponen una desterritorialización de su campo de acción, al instar a las compañías aéreas para que envíen los datos de sus pasajeros mediante la elaboración de un fichero detallado y la toma de huellas de todos los pasajeros que entren en su territorio. En una dirección parecida ha entrado la misma Unión Europea, al aceptar las reglas de la OACI (Organización de la Aviación Civil Internacional), que impone a sus 190 estados miembros una serie de reglas entre las que destacan las normas comunes para la documentación de viaje, con capacidad de ser leídos por maquinas idénticas, que contendrán información biométrica individual, incluso de niños.

El Sistema *de Información Shenguen,* consecuencia del acuerdo del mismo nombre de 1990, ya fijaba una forma de retener datos sobre los ciudadanos de países fuera de ese tratado dentro de las fronteras, como mecanismo de control. El *Eurodac*, de 2003, abundaría en esa perspectiva de recogida de datos individuales, tomando las huellas digitales de peticionarios de asilo y de inmigrantes "ilegales" para su comparación.

En 2009, el VIS, Sistema de Información sobre Visados, pretende convertirse en la mayor recopilación de información mundial sobre visados biométricos (con fotografías y huellas primero). Abundando en la gestión de los datos privados[483], la Directiva Europea 2006/24/CE[484], incorpora aspectos básicos de la *Patriot Act* al imponer a las compañías de telecomunicaciones la obligación de conservar por un periodo de entre 6 a

---

[483] Martínez, P. *Los peligros de la tecnología*. Recurso electrónico en: http://www.internautas.org/html/5670.html

[484] La Polémica Directiva Europea 2006/24/CE sobre vigilancia: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=ES&reference=P6-TA-2009-0360

24 meses numerosos datos de comunicaciones telefónicas, incluida información sobre la ubicación, y de Internet[485]. Mediante esta fórmula se consigue también transponer a los parlamentos nacionales y sacarla de un debate que podría ponerla en cuestión; y de este modo, España sería uno de los primeros Estados en incorporarla, mediante la Ley sobre Conservación de datos de las Comunicaciones Electrónicas de 18 de octubre de 2007.

La combinación de bancos de datos de procedencias diversas puestos a disposición de los organismos de control estatal, o al menos la referencia que los estados mantienen, puede ser una de las piezas críticas en este momento dada la privatización progresiva de este campo también, como sabemos por el caso del ejército mercenario de *Blackwater*, ahora denominado *XE*[486] , que tiene a su disposición información directa por parte de las agencias de información norteamericanas, dado su papel "gestor" de la seguridad en lugares como Irak[487]. En efecto, esta cesión de derechos por parte de los estados a gestores privados de información, mediante contratas para la elaboración de planes concretos de instauración de procesos de vigilancia, como el caso de la TIA a la empresa Syntec, filial de Sagen Securite, líder en sistemas multibiométricos, por parte de Donald Rumsfeld, también responsable del caso anterior[488], son tan solo ejemplos de los que vamos teniendo constancia.

---

485 Directiva Europea sobre la retención de datos: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0420:FIN:ES:PDF

486 Scahill, J. *Blackwater, el ascenso del mayor ejército mercenario del mundo*: http://blackwaterbook.com/

487 entrevista a J. Scahill.: http://www.democracynow.org/2007/3/21/part_ii_blackwater_the_rise_of traducción en castellano: http://www.rebelion.org/noticia.php?id=48803

488 Preuss-Laussionotte, S. *La democracia ante los riesgos de la mundialización de las*

Un efecto que acompaña esta oleada de seguridad y recogida de datos particulares son las que las propias compañías aseguradoras y de seguridad privada llevan adelante por su cuenta. En ese sentido, las nuevas formas de vigilancia mediante geolocalización, empleando teléfonos móviles, cuya señal es triangulada, o mediante los GPS, suponen un paso más en el control de personas, aplicadas en principio a vehículos de empresa y a la vigilancia judicial en principio, pronto han ido extendiéndose, como el caso de la empresa *Orange*, que, en Francia, ofrece la posibilidad de conocer la ubicación de los teléfonos móviles contratados, con excusas comerciales iniciales como la de conocer dónde están los hijos. Este resulta un caso mucho más escandaloso que el reconocido socialmente, como en los casos de vigilancia de condenados, sobre todo en casos de maltrato, con las alarmas de proximidad o localización permanente. La progresión en los dispositivos de vigilancia con persistencia en su conexión se encuentra en su momento inicial aunque su expansión apenas puede ser refrenada por iniciativas para salvaguardar la privacidad.

Chips de seguimiento permanente

El siguiente paso en la captación de datos personales podemos encontrarlos en la expansión de los Chips de radiofrecuencia (RFID), dispositivos variados que cada vez se instalan en más elementos de consumo, comenzando por tarjetas de crédito e identificación para pasar a ser uno de los elementos de seguridad y seguimientos de productos en venta y almacenaje. Aunque el elemento que más posibilidades está mostrando son los denominados Chips de radiofrecuencias "activos", compuestos por un pequeño Chip con un microprocesador integrado capaz

---

bases de datos. En El estado del mundo 2009. Akal, Barcelona 2008.

de activarse mediante la radiación electromagnética que puede emitirse en zonas concretas para estimular el registro de los datos almacenados en este.

El gran salto entre estos lectores frente a los tradicionales (Pasivos), es su enorme radio de acción frente a los precedentes, que pasan de los escasos centímetros que emplean ciertos cajeros y unidades lectoras, como las empeladas por el *DNI electrónico* o los lectores de ciertos comercios, a la activación inadvertida a decenas de metros del puesto de lectura[489]. Este tipo de identificación, transciende sobremanera estos procesos anteriores, al ser capaz de identificar individualmente cada Chip, y al producto y usuario concreto, sin ser desactivado al realizar la compra, podrá ofrecer una información completa de los hábitos de consumo, los itinerarios y las preferencias personales de cada persona que, con el tiempo, puede portar múltiples de estos Chips sin ser consciente de ello. Los primeros pasos en la expansión de este tipo de dispositivos ya se han iniciado, con ejemplos como el del pasaporte biométrico francés, desde 2006, o los pases de peaje en nuestras autopistas y ciertos elementos antirrobo en vehículos de gama alta. De cualquier modo, el componente más inquietante de esta nueva tecnología sutil es su tremenda expansión en los últimos años, sobre todo en el terreno comercial, y la posibilidad de que los datos que se emitan puedan ser susceptibles de ser integrados en bases de datos de computación global, como promete el siguiente salto a la Web 3.0[490]. Mediante la integración de todo el procesado de datos de lectores discretos y desatendidos pero integrados en bases de datos generales se puede llegar a extremos de control completo de la población

---

[489] . Alberganti, M. *Los Microprocesadores contra las libertades*; en El estado de Mundo 2009. Akal. Barcelona. 2008

[490] Alberganti, M. http://www.smallbrothers.org/

por parte de organizaciones privadas y empresas si no se legisla en este sentido y se establecen parámetros claros con los que estos dispositivos pueden identificarse[491]. Estas tecnologías de radiofrecuencia han adquirido en estos años una especial difusión a raíz de la expansión de las tecnologías móviles. Los Chips NFC (Near Field Communication-Comunicación de corto rango) se han extendido a lo largo de múltiples dispositivos hasta convertirse en uno de los estándares más utilizados. Esta extensión entre medios de pago y comunicaciones de corto rango, también suponen una integración en el seguimiento de usuarios y patrones en la que todavía no está clarificado su limitación legal[492]. Aunque teóricamente, los rangos de acción de estas frecuencias apenas alcanzan unos centímetros, ya se han realizado pruebas de concepto por la comunidad hacker en los que se han podido acceder a chips de forma externa y alejada.

[491] Informe de la Real Academia de Ingeniería Británica de Ingeniería sobre el uso incontrolado de radiofrecuencia

[492] *NFC Fórum*, es la organización creada en torno a la elaboración de estándares para esta tecnología de radiofrecuencia: http://www.nfc-forum.org/aboutus/

El espionaje masivo ciudadano: Un Gran Hermano global y privado

Una de las cuestiones que más controversias han levantado a lo largo de la primera década del presente siglo ha sido el establecimiento por parte de los diferentes gobiernos de mecanismos de vigilancia masiva ciudadana. La parte esencial de este escándalo será la progresiva privatización de los mecanismos de vigilancia en favor de contratas privadas[493]. Sin embargo, ni las revelaciones de WikiLeaks ni de Edward Snowden, como veremos en el siguiente capítulo, han modificado sustancialmente la forma en la que los programas de ciberseguridad son subcontratados por estamentos de seguridad e inteligencia de las diferentes naciones[494]. EEUU ha sido en este sentido pionero en la capacidad de establecer relaciones con la empresa privada. La investigación llevada a cabo por el periodista Barret Brown y su relación con elementos de algunas organizaciones de Anonymous, culminarán con su acusación de colaboración terrorista y posterior encarcelamiento. El mensaje para el periodismo de investigación y la confidencialidad de las fuentes, quedará de este modo confortada con una realidad en la que el peso de dichas contratas puede llegar a altas cotas de contorsionismo legal en la evasión de responsabilidades y la persecución de agentes hostiles"[495].

---

493 Greenwald, Glenn - *Snowden. Sin un lugar donde esconderse*. Ediciones B. Barcelona. 2014

494 Assange, J. *Cypherpunks. La libertad y el futuro de internet*. Deusto. Madrid. 2014.

495 Sobre la detención de Barret Brown, existe una campaña abierta por su liberación: https://freebarrettbrown.org/

Las sucesivas revelaciones que han llegado de la mano de las grandes filtraciones y un esquema de entre activistas de alerta, han conseguido establecer una línea de reconstrucción de la mayor parte de los programas de vigilancia en la red existentes. La tendencia general a la vigilancia e integración de datos biométricos de ciudadanos en grandes bases de datos para un posterior análisis multidisciplinar no ha dejado de crecer. En este sentido, no solo contratas y agencias vinculadas a los gobiernos sino grandes compañías de internet han comenzado a procesar e integrar datos de sus usuarios. La cuestión se amplifica con la adquisición de datos biométricos obtenidos de las fotografías que diferentes usuarios suben a sus respectivos servicios. Como ya vimos, Facebook, ha planteado en sucesivas ocasiones, la integración en su red social de la identificación de usuarios a lo largo del alojamiento que integra sus datos. El siguiente paso en la integración de datos es la de la adquisición de datos procedentes de dispositivos de videovigilancia [496] . En diversas ocasiones se ha planteado el papel de los circuitos de videovigilancia han tenido. Los atentados en el maratón de Boston, en abril de 2013, traerían al primer plano informativo la capacidad de acceso generalizado a la captación de datos mediante sistemas de vigilancia exterior[497]. De forma acelerada, el

---

[496] Periano, M. *El pequeño libro rojo del activista en la red*. eldiario.es libros. Madrid. 2015

[497] Información sintetizada por la Wikipedia acerca de los atentados de Boston de 2013. Al acceder a fuentes periodísticas puede ser la mejor referencia, al contener citas de enlaces no permantentes: thttps://es.wikipedia.org/wiki/Atentado_de_la_marat%C3%B3n_de_Boston

18. Sobre los sistemas de videovigilancia, escribí varias colaboraciones periodísticas. Las más reciente en Rebelión titulado *Tu cara no es anónima*": http://www.rebelion.org/noticia.php?id=200343

Véase también: *El avance de la Videovigilancia sin garantías ciudadanas*: http://www.eldiario.es/turing/vigilancia_y_privacidad/videovigilancia-analisis-biometrico-garantias-ciudadanas_0_149435381.html

FBI llevaría adelante un sistema denominado NGI (Next Generation Identification) encargado a la contrata Lockheed Martin, para poder integrar los datos captados por todos los sistemas de vigilancia biométrica. El sistema saca partido de orígenes precedentes de datos para integrarlos en el nuevo sistema, por lo que no descarta las fichas policiales anteriores. Así, la gran base de datos que el FBI está elaborando es en la actualidad uno de los más potentes mecanismos de control de toda la historia. En este sentido, trabajan para ampliar los datos de huellas dactilares añadiendo información relativa a escáneres de palma de mano, del iris ocular y sobre todo de fotografías y videos. Uno de los puntos que más suspicacias ha levantado es precisamente ese nuevo método de reconocimiento facial mediante captación de imágenes por circuito de videovigilancia, un sistema puesto en funcionamiento pleno en 2014 y mediante el cual podemos ser ubicados sobre la marcha en cualquier lugar donde esta red de cámaras capte nuestra imagen[498].

En EEUU, la National Defense Authorization Act (NDAA) ofrecerá un marco lo suficientemente ambiguo, para permitir con la excusa de la lucha global contra el terrorismo la suspensión de libertades ciudadanas y la retención de individuos sin acusación formal[499]. El mismo rango de indeterminación permite en esencia que cuestiones que deberían seguir un itinerario judicial sean desviadas hacia el Departamento de Defensa. De este modo se amplifica el rango de actuación de los organismos vinculados a defensa y sus contratas, que al amparo de la persecución del terrorismo

---

[498] El sistema *Next Generation Identification* (NGI) integra todos los sistemas de captación de datos existentes para su procesado e identificación en tiempo real. Desde finales de 2014 se encuentra operativo, con un rango de error del 20%: https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/ngi2

[499] La *National Defense Authorization Act* (NDAA), es una polémica ley que permite un amplio rango de intervención por parte de las autoridades respecto a ciudadanos: https://www.govtrack.us/congress/bills/112/hr4310/text

pueden establecer mecanismos de vigilancia masiva cuyos datos podrán luego emplearse convenientemente. La experiencia nos enseña que este caso puede volver a ser utilizado como excusa de la "seguridad" para que elementos ajenos a las agencias estatales atesoren datos so pretexto de ceder luego estos y ponerlos a completa disposición de los estados[500].

La gran profusión de programas de vigilancia masiva revelados a lo largo de las filtraciones en primer lugar de WikiLeaks pero especialmente a lo largo de 2013 con los datos extraídos por Edward Snowden desvelaran sin espacios de duda el gran negocio creado en torno a los sistemas de captación y procesado de datos[501]. Acompañando a estas revelaciones, la constatación de que estos programas se enfocaban a un espionaje generalizado de la ciudadanía en general gracias a la oportunidad ofrecida por las legislaciones antiterroristas [502] . *PRISM*, *XKeyscore* [503] y la posibilidad de un post procesado de la minería de datos ofrecidos por programas como *Boundless Informant* serán solo ejemplos de la multiplicación de programas en concurrencia y competencia en muchas ocasiones[504]. La valoración de

---

[500] . VVAA. *The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008), ISBN 0-262-54196-3 http://www.opennet.net/accessdenied/

[501] Listado de sistemas de vigilancia masiva internacional mantenida por la fundación Wikipedia: https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects

[502] Greenwald, G. *Snowden. Sin un lugar donde esconderse*. Ediciones B. Barcelona. 2014. La actividad de la fundación ha sido al respecto muy destacada al permitir alojar en sus servidores buena parte de la documentación hecha pública.

[503] Edward Snowden publicaría las especificaciones del programa X-Keyscore, documento que actualmente puede ser consultado en: https://en.wikipedia.org/wiki/File:XKeyscore_presentation_from_2008.pdf.La actividad de la fundación ha sido al respecto muy destacada al permitir alojar en sus servidores buena parte de la documentación hecha pública

[504] El sistema de minería de datos Boundless Informant, permite el acceso y procesado de los datos obtenidos mediante sistemas de espionaje: http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-

esta carreara por la contrata de servicios de las agencias policiales, de Inteligencia y de defensa de EEUU nos deja un panorama del grado de perversión al que ha llegado el sistema responsable de la seguridad en esta democracia y el poder que las diversas contratas tienen a la hora de establecer y buscar financiación para unos programas completamente privatizados[505].

EEUU no será un elemento aislado en la vigilancia masiva de ciudadanos. Más allá de programas con una larga trayectoria, como el ya conocido Echelon, multitud de aliados y la mayor parte de países occidentales han llevado adelante sus particulares sistemas de vigilancia y procesado de datos. El alcance de sus propias redes en sistemas como TEMPORA, en colaboración con el GCHQ, la agencia de inteligencia y espionaje británico, que pondría en manos de la NSA norteamericana, los datos captados a través de la intervención de los cables de fibra óptica de buena parte de las comunicaciones europeas, que tienen como enlace territorio británico[506].

En este apartado, la UE tampoco ha permanecido al margen y fruto de una política cada vez más restrictiva, a cargo de unos estamentos cada vez más plegados a una ideología neoconservadora. De forma

---

global-datamining

[505] Sobre el asunto de las contratas privadas, Barret Brown, publicaría bastantes datos extraídos de fuentes cercanas a Anonymous. Existe poca información *al respecto en castellano. En 2013* compuse un artículo previo a su definitiva acusación*: Quién es Barrett Brown, el periodista especializado en espionaje que está en la cárcel*: http://www.eldiario.es/turing/privatizacion-espionaje-periodista-Barret-Brown_0_150485289.html

[506] VVAA. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), ISBN 0-262-51435-4 http://www.access-controlled.net

paralela al control antes explicado de la directiva de *Shengen*, que prevé la retención de ciudadanos se han adelantado mecanismos de control ciudadano mucho más avanzados que un control fronterizo y de desplazamientos[507]. Uno de los sistemas de adquisición y almacenado de datos vendrá por parte de la directiva de retención de datos , que obliga a las operadoras de Internet a retener los datos de conexión de sus usuarios, por periodos de seis a 24 meses, según el desarrollo legislativo de cada nación. Esta herramienta ofrece en combinación con ciertos desarrollos legislativos como los casos inglés o francés, la capacidad fiscalizadora a estas empresas que son las que deben controlar los tráficos de datos de sus usuarios para poder determinar si estos descargan efectivamente contenidos cubiertos por legislaciones de protección de derechos. En caso afirmativo, a los usuarios serán sancionados e incluso privados de su conexión a Internet. Son las conocidas como ley de los tres avisos y la *Hadopi*, ambas muy discutidas en sus respectivos países al permitir que las operadoras auditen la conexión a internet de sus usuarios. Como veremos, la reacción será la proliferación de redes cifradas y accesos con diversos métodos de ofuscación y ocultación de las conexiones[508].

A pesar de lo expuesto, la herramienta de control más polémica de la UE será INDECT (*Intelligent information Systems supporting observation, searching and detection for security of citizens in urban environment)*, una herramienta que en principio integraría el rastreo de la videovigilancia para establecer patrones de conducta "sospechosa". El

---

[507] Privacy International: *¿Quién vigila al vigilante?.* El Informe de Privacy internacional es un gran recurso a la hora de conocer los métodos de vigilacia masiva actuales. Se encuentra disponible en: https://www.privacyinternational.org/?q=node/351

[508] Sobre la evasión de la censura en Internet la organización Floss ha publicado una completa guía en formato de Libro electrónico de muy recomendable lectura: https://howtobypassinternetcensorship.org/es.html

proyecto, integra herramientas de control y catalogación de conductas en la red, mediante el control de contenidos de redes P2P, foros o webs. Se trata por tanto de un sistema que excede el ámbito de la legalidad y que no respetaría la ley de protección de datos y muy discutiblemente otras en los aspectos de derechos esenciales[509]. La realidad del proyecto ha movilizado a las asociaciones de derecho y activistas de Internet ante esta escalada en la vigilancia ciudadana indiscriminada. Para establecer esto patrones de conducta y los perfiles individuales hasta llegar a declarar conductas sospechosas, se está auditando a todo el conjunto de la ciudadanía, sus comunicaciones, su vida privada cada vez que pase delante de zonas videovigiladas integradas en la red y en general cada uno de nuestros rastros ya no solo estrictamente tecnológicos o al menos producidos en nuestra conexión. INDECT es un proyecto civil, que deben gestionar policías y medios judiciales de las diversas naciones que forman parte del proyecto, por tanto la vigilancia adquiere un carácter todavía más preocupante al enfocarse en un seguimiento de corte policial de ciudadanos sin enlace con estrategias de seguridad de otro tipo, tan convenientemente empleadas en tiempos recientes[510].

El desarrollo paralelo en las cuestiones militares cuenta con su desarrollo de rastreo masivo, denominado OSEMINTI (*Infraestructura de Inteligencia Semántica Operacional)*. Adoptado por el Consejo de ministros de la UE e implantado por los ministerios de defensa de Francia, Italia y Francia, es uno de los proyectos estrella de la Agencia Europea de

---

509 INDECT: http://www.indect-project.eu/

510 Informe sobre la adquisición de datos biométricos y su gestión a cargo de Privacy International: https://www.privacyinternational.org/?q=node/48

Defensa[511]. La envergadura del proyecto es una de las explicaciones de esta colaboración entre estados para el espionaje civil. En esencia, el sistema es una réplica del que empleara durante años el FBI estadounidense, denominado *Carnivore*, que cuenta con la capacidad de procesar una ingente cantidad de datos y relacionarlos para aprender pautas y ser capaz de gestionar ciertos contextos. El conocimiento que adquiere este sistema responde a un patrón semántico, no solo en torno a palabras sino a significados dentro de las comunicaciones, muy en consonancia con la gestión de Big Data para sustituir a personas en el tratamiento y catalogación de datos. Así se va a permitir unificar las informaciones de diversos orígenes de vigilancia masiva para que sean filtradas por la máquina de OSEMINTI y así ofrecer resultados que concuerden con patrones sospechosos. La clave de todo este proyecto es por tanto la interceptación masiva de tráfico de información por parte de usuarios sobre los que no pesa orden judicial, sospecha ni investigación policial. Para ello se apoya en la regulación de retención de datos por parte de los operadores de Internet que ya hemos mencionado anteriormente. El argumentario en su defensa, tras la polémica de su revelación también acudió a lugares comunes de nuestro siglo, como la defensa contra el terrorismo internacional[512].

---

[511] Agencia Europea de defensa: http://www.eda.europa.eu/ Bajo el paraguas de la reciente estrategia europea de ciberdefensa, aprobada en noviembre de 2014, integrarán sus investigaciones dentro de este marco: http://www.eda.europa.eu/our-work/projects-search/cyber-defence

[512] Existe una extensa información sobre la vigilancia y la privacidad a cargo de la asociación en defensa de las libertades *La Quadrature du net*: http://www.laquadrature.net/en/Privacy

El espionaje español

Por si misma, España también cuenta con su propio sistema de vigilancia civil, basado en las escuchas telefónicas denominado SITEL[513]. El sistema, ha sido uno de los más expuestos mediáticamente, en parte producto de una interesada disputa acerca de su origen, aunque lo cierto es que ningún cambio de gobierno puso sobre la mesa su reforma o cancelación. En esencia, se trata de un sistema de captación y escucha de telefonía a cargo del Misterio de Interior y que comparten la Policía Nacional, la Guardia Civil y el Servicio de vigilancia Aduanera. Una de las ocasiones en las que volvería a tener relevancia sería precisamente en el *caso* de la detención de la supuesta cúpula de Anonymous en España en 2011 [514] . Como se demostraría, tan solo un grupo de activistas habituales de grupos de chats vigilados por el sistema y que se arrogaban algunos ataques DDoS (denegación de servicio saturando servidores de peticiones, algo que no requiere unos conocimientos muy especiales, dado que tan solo se necesita instalar una herramienta llamada LOIC y escribir la IP de la víctima[515]. El procedimiento sería largamente usado contra la SGAE , partidos políticos y operadores como Telefónica en

---

[513] SITEL ya sería discutido desde sus orígenes en 2009, antes de su popularización en 2011 al calor del debate parlamentario. La asociación de internautas discutiría fuertemente sobre su conveniencia y la gestión legal de los datos: http://www.internautas.org/html/5711.html

[514] Sobre el caso de la detención de la supuesta cúpula de Anonymous, quedarían muchas cuestiones pendientes y por aclarar, tanto por lo truculento y mediático del asunto como por las consecuencias reales: https://www.diagonalperiodico.net/libertades/26983-caso-anonymous-cuatro-anos-despues.html

[515] Para conocer la simpleza del uso de LOIC y como es una herramienta muy extendida en ciertos foros la entrada de la Wikipedia es muy interesante. Ahora mismo, la mayor parte de proveedores cuentan con sistema de balanceo de cargas para mitigar los ataques DDoS, que tienen cada vez menores consecuencias: https://es.wikipedia.org/wiki/Low_Orbit_Ion_Cannon

sucesivas acciones de protesta y no tenía más consecuencias que la caída de los servidores atacados[516]. La realidad de SITEL también ha estado siempre en discusión por la constante sospecha de vigilancia al activismo, hecho que no solo revela el caso de la supuesta cúpula de Anonymous sino que sitios como Nodo50, un portal que da servicios a ONG y colectivos sociales, han podido atestiguar en sus máquinas[517].

La reciente aparición de estamentos de seguridad españoles como clientes de la empresa italiana de espionaje *Hacking Team*, tan solo ha sido el último capítulo de una larga serie de revelaciones al respecto. Lo más destacado de este último asunto es que esta empresa se dedicaba a la venta de vulnerabilidades y agujeros de seguridad todavía no descubiertos en la comunidad hacking ni publicados para poder proceder a explotarlos con diversas herramientas ofensivas que habían sido convenientemente simplificadas para manos menos expertas con un software denominado RCS (Remote Control Systems). La empresa se dedicaba a una labor parecida a la que veremos del mercado negro pero enfocado a gobiernos mediante procedimientos de espionaje ilegal con técnicas poco éticas[518]. La empresa ya estaba en el ojo de muchos activistas por su reconocida venta de capacidades de espionaje a dictaduras. La puesta en público de dicha información llegaría en julio de 2015 por una vía de un hackeo a la propia empresa que culminaría con la exposición de 400 Gb de información interna, facturas, software y datos de

---

[516] Sobre el espionaje a sitios alojados por Nodo50 y los sucesivos ataques a su infraestructura: http://www.nodo50.org/criminalizacion_mov_sociales/nodo50/

[517] Nodo50 llegaría a rastrar las IPs de quienes accedían a sus equipos de forma remota e iniciaría una campaña de identificación y condena: http://losvigilantes.nodo50.org/infospanish.htm

[518] El escándalo de Hacking Team ha salpicado a varias naciones, España entre ellas con tres contratos. Las herramientas están descritas aqui http://www.elladodelmal.com/2015/07/hacked-hacking-team-espana-brasil.html

clientes incluidos. El Centro Nacional de Inteligencia de España será uno de los que aparezca en esa lista de clientes que adquieren varias aplicaciones para explotar vulnerabilidades tipo *Zero Day* (no publicadas ni conocidas) y vuelve a comunicar los extremos del Black Hacking, los que se dedican a la delincuencia, y los estamentos gubernamentales[519].

Toda esta profusión de proyectos de espionaje y captación de datos privados nos sitúa cada vez más en un sistema de restricción de las libertades ciudadanas[520]. Mantener a la ciudadanía en un estado de vigilancia permanente por la eventualidad de un comportamiento delictivo o terrorista no es solo un atropello a las libertades sino una auténtica declaración de intenciones de quien tan solo lo sugiera. La criminalización preventiva asaltando la privacidad se ha extendido a lo largo del presente siglo de una manera imparable. La pesadilla orwelliana puede finalmente ser ejecutada por parte de los estados que finalmente han conseguido tener los recursos tecnológicos suficientes como para llevarla adelante como si de un manual de uso se tratara. El acceso y uso democrático y la negación a la permanente vigilancia de las personas resulta en nuestros días un pilar fundamental de la democracia y una divisoria real y tangible de quien es quien en todo el proceso. Precisamente de la rebelión contra este asalto a la privacidad y los instrumentos de defensa colectivo e individual tratarán los siguientes capítulos.

---

519 *The Vergue* sería una de las primeras publicaciones en analizar los datos robados a la empresa Hacking Team: https://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers

520 Privacy Internacional y Amnistía internacional han publicado un informe sobre el estado de la cuestión de las revelaciones de Edward Snowden titulado "*Two Years after Snowden. Protecting Human Rights in an age of mass surveillance*". Disponible en: https://www.privacyinternational.org/?q=node/591

4.2 WikiLeaks, Whistleblowers, y grandes filtraciones

En noviembre de 2010, se produjo un acontecimiento a nivel global que trastocaría de forma definitiva la forma de entender la sociedad de la información y la manera en la que hasta ese momento nos desenvolvíamos en la red. Una organización sin ánimo de lucro, denominada WikiLeaks[521] filtró a la prensa internacional una colección de 251.187 comunicaciones entre el Departamento de Estado de Estados Unidos y sus embajadas por todo el mundo. Se trataba de la mayor filtración de documentos secretos diplomáticos de la historia, e inmediatamente desencadenó una crisis global que será recordada con el nombre de *Cablegate*. Una secuencia a lo largo de 2010, en la que se publicarían los denominados Diarios de la guerra de Afganistán, en julio y los registros de la guerra de Irak, junto con los cables diplomáticos. El grueso de la información publicada comprometería a la diplomacia estadounidense, tanto por sus métodos como por la relación con socios y aliados. La abrumadora cifra de lo expuesto, con medio millón de registros sobre ambas guerras y 250.000 comunicaciones diplomáticas, no dejaba lugar a dudas a propósito de la autenticidad de las fuentes.

El nombre compuesto *wiki-leaks* hace referencia tanto al término hawaiano comúnmente adoptado entre usuarios de red para denominar diferentes ámbitos organizativos para consultar documentación[522], como al término anglosajón que hace referencia a la filtración o fuga, en este caso

---

[521] El sitio principal de WikiLeaks sigue actualmente activo en: https://wikileaks.org/

[522] Padilla, M. *El kit de la lucha en Internet*. Traficantes de sueños ed. Madrid. 2012

respecto a información confidencial. Lo más interesante de la organización, es su forma de funcionamiento, pensada para garantizar el secreto de la identidad de la fuente, así como una purga de información personal que pudiera poner en peligro a individuos concretos. En clave interna, su funcionamiento se inició en diciembre de 2006, con un equipo plurinacional liderado por el exhacker australiano Julian Assange. En los tres años que van desde la fundación de organización hasta la publicación de este archivo, WikiLeaks se había dedicado a cooperar con una salida democrática para Kenia y asentar las bases de una red de confidentes. Muchas de sus filtraciones, al tener un alcance limitado y dedicarse a temas de corrupción no alcanzarían la dimensión posterior de los datos que obtendría a partir del *cablegate*. Así revelaciones en torno a la financiación de la *Cienciología*, el manual de Microsoft para espiar a sus usuarios, que publicara la web Cryptome.org y terminaría llevando a su cierre temporal o los correos de la controvertida Sarah Palin marcarían los inicios de la web de filtraciones[523]. Pero el acontecimiento que pondrá en el mapa a la organización será la ingente revelación de los atropellos norteamericanos en Irak y Afganistán; los llamados *Diarios de Guerra*[524].

En parte estos documentos revelaban las formas en las que se espiaba y en que la diplomacia internacional gestionaba sus asuntos en su cara no pública[525]. El asunto llevó a la indignación a muchos "aliados" que veían como con total sinceridad se opinaba respecto a mandatarios y

---

[523] Assange, J. *Cypherpunks. La libertad y el futuro de internet*. Deusto. Madrid. 2014

[524] Los llamados *diarios de guerra* sobre Irak y Afganistán siguen disponibles, ordenados y catalogados por diferentes categorías en: https://warlogs.wikileaks.org/

[525] Dromscheit-Berg, D. *Dentro de WikiLeaks. Mi etapa en la web más peligrosa del mundo*. Roca. Barcelona. 2011

dirigentes y se fijaban estrategias cuando menos espurias. Aun así, la parte más escandalosa de esta filtración inicial a una serie de diarios internacionales elegidos, *The Guardian, The New York Times y Der Spiegel,* se iría produciendo de forma escalonada, sobre todo debido a la ingente cantidad de información que necesitaba ser procesada e interpretada antes de convertirse en noticia. Estos diarios ya tenían acceso a las primeras listas de información confidencial sobre la guerra de Afganistán que ascendían a un total de 91.731 documentos, datados entre los años 2004 y 2009 y a los llamados *Diarios de guerra de Irak,* con un total de 391.831 documentos desde unos meses antes. Desde el 22 de octubre de 2010 estos medios contaban con dichas informaciones. La documentación trataba de forma extensa a propósito de cómo se dejaban conscientemente sin investigar asuntos relacionados con informes acerca de torturas e incluso asesinatos perpetrados tanto por la policía iraquí como por el propio ejército estadounidense. El relato de la situación de los presos y la connivencia de los destinatarios de dichas informaciones. El grueso de esta información sería publicado en la página de la organización al tiempo que se remitía a un grupo mayor de medios entre los que destacan *The Guardian, The New York Times, Le Monde, DerSpiegel, El País, Al Jazeera* o el *Bureau of Investigative Journalism* , con la intención de que estos puedan divulgarlos en sus correspondientes ediciones digitales. De cualquier forma, ya por otros medios la opinión pública internacional tenía una imagen bastante clara del papel de las alianzas formadas tanto en Afganistán como en el caso de Irak. La parte menos conocida del asunto de cómo actuaba la inteligencia estadounidense era el asunto que saltaría un mes después con el *cablegate*[526].

[526] Un relato completo y detallado de la trayectoria de las filtraciones de WikiLeaks puede leerse en la propia páginade WikiLeaks: https://wikileaks.org/About.html

La reacción al *cablegate*

Las revelaciones del 22 de noviembre de 2010, terminarían por poner en evidencia la política y la diplomacia de buena parte de las democracias occidentales y el papel tan adjetivable de la estadounidense. Un grueso de 251.187 comunicaciones supuso una carga excesiva para cualquier grado de relativización o matización por parte de los que originaban esta documentación. Pocos gobiernos de las naciones de las democracias de corte occidental quedaban limpios[527].

En lo que respecta a España, se hacían claras menciones al interés por dar carpetazo al caso del cámara español José Couso, asesinado en Bagdad el 8 de abril de 2003 por disparos de un tanque estadounidense así como al caso de los traslados de supuestos terroristas internacionales a la cárcel de Guantánamo en vuelos ilegales que realizaron escalas en suelo español sin consentimiento expreso[528].

La reacción del gobierno norteamericano supuso un caso paradigmático de la doctrina de la ocultación. Acusar a las fuentes en primer lugar de traidoras, matizar y negar la mayor parte de las pruebas y tratar de asfixiar los mecanismos de financiación del medio. Así uno de los primero pasos será la presión a los medios de pago y financiación de WikiLeaks. En este caso el portal de pagos por Internet, *PayPal* será el

---

[527] El grueso de la documentación del denominado Cablegate, puede ser consultado en la propia página de WikiLeaks o descargado el grupo de la documentación, ya catalogada desde varios enlaces y en varios formatos para su consulta: https://wikileaks.org/cablegate.html

[528] Animo a la lectura detallada del conjunto de datos de 2006 a 2010 sobre España. La mayor parte del relato informativo puesto frente a una realidad diplomática y unas intenciones no declaradas: https://wikileaks.org/wiki/Category:Spain

primero en plegarse a las presiones del gobierno norteamericano para cancelar la cuenta de donaciones del medio. Seguirán Visa y MasterCard, entidades mundiales de tarjetas de crédito y pagos, que suspenderán todas las transferencias de fondos a esta asociación[529]. Junto a estos Amazon, bloqueará el uso de sus famosos servidores de datos y twitter pasa a suspender varias cuentas y retira de las listas de *Trending topic* (tendencias del día) la etiqueta *#freeassange* (forma principal de identificar y agrupar publicaciones en esta red social). El papel de estas compañías, completamente serviles a una censura injustificada, marcara el devenir de los acontecimientos que sigan y será causa de una ruptura que medios y colectivos civiles que mantenían ciertas simpatías con la política de empresas de Internet como Twitter o Google. Como ya hablamos cuando Stallman afirmaba que el comportamiento del software privativo debía asimilarse al malware, la extensión de esta idea, tras la constancia del espionaje y el pliegue de estas compañías antes las exigencias del gobierno norteamericano terminarán por asentar esa idea entre colectivos cada vez más extensos de la población[530]. La nube comenzará a cuestionarse y el cifrado dejará de considerarse "cosa de *geeks*" para pasar a ser instrumento básico de colectivos como el de periodistas[531].

Uno de los aspectos más inquietantes del asunto, ya en 2011, sería la colaboración de las grandes corporaciones de Internet en

---

[529] Sobre el bloqueo a las donaciones de WikiLeaks, la propia página publicaría un informe detallado de la situación financiera a la que fue sometida y las fuentes de su financiación. La documentación es pública y se encuentra en la misma página: https://wikileaks.org/Banking-Blockade.html

[530] Compañías como Twitter, ante la polémica servida en su propia red acerca de la censura, publicaría incluso un desmentido oficial al respecto en su blog: http://blog.es.twitter.com/2010/12/sobre-los-temas-del-momento.html

[531] Padilla, M. *El kit de la lucha en Internet*. Traficantes de sueños ed. Madrid. 2012

estos casos de espionaje. El propio Assange, asegura que en junio de 2011, mantendría una entrevista con Eric Schmidt, el presidente ejecutivo de Google[532], que este considera como el de la compañía más influyente del mundo, de la que extraería las tesis generales de este respecto a la misión de esta empresa en sintonía con los intereses "de estado" de EEUU. Tales tesis serían ampliamente confirmadas tras el bloqueo efectivo de otras grandes corporaciones. Poco después se irán conociendo los casos de Amazon, Apple, Microsoft y Yahoo! las puertas traseras de entrada para agencias de espionaje, como el caso PRISM, o las cesiones de datos no siempre justificadas con una base legal. Por supuesto esas bases ya habían sido suficientemente matizadas desde la *Patriot Act*, pero ahora se trataba de un control paralegal, llevado a cabo por compañías privadas, los más de los casos contratas de agencias gubernamentales, como sobradamente documentaría Edward Snowden, apenas dos años después. Así las revelaciones de WikiLeaks no solo estaban poniendo en entredicho la política del gobierno de Estados Unidos, sino que empezaba a resquebrajar la imagen y la confianza de las grandes compañías de Silicon Valley. Efectivamente, la actitud servil y cuando menos equidistante de Google, Yahoo! o Microsoft en cuanto al acceso a sus cuentas de correos de usuarios abrirá un cuestionamiento público sobre cómo puede ser libre una red supeditada casi por completo a compañías privadas de EEUU[533].

Por otro lado, los movimientos cívicos centrados en las libertades de Internet verían cómo tomaba más relevancia hasta pasar a un primer plano como nunca antes habían alcanzado. Extensas campañas de

---

[532] Assange, J. *Cuando Google encontró a WikiLeaks*. LMD-Clave Intelectual. Madrid. 2014

[533] Assange, J. *Cypherpunks. La libertad y el futuro de internet*. Deusto. Madrid. 2014

la *Electronic Frontier Foundation* (EFF), afectarán a grandes proveedores de servicios de EEUU, acusados de colaborar con el gobierno estadounidense en tareas no reveladas de espionaje a usuarios de todo el mundo, con unos métodos mucho más sofisticados que los ya conocidos, como la red Echelon[534]. Una red que sigue activa hoy en día y aportando su particular grano de arena a la red de intervención global que compone todo el marco del espionaje[535].

La necesaria colaboración de empresas como Yahoo!!, Apple, Google, Facebook o Twitter, en la identificación de usuarios, no ya por la condición de una orden judicial sino por la petición expresa de las agencias de seguridad norteamericanas colocará en una posición comprometida a estas compañías. Su primera reacción sería negar esa colaboración, máxime cuando muchas de estas exigen un informe judicial detallado para revelar datos de sus usuarios a países como España. Al poco iniciarían una campaña conjunta en defensa de las libertades en internet, muy en sintonía con las que organizaciones cívicas llevaban adelante y que incluía a estas empresas entre quienes no gestionaban claramente los datos de sus usuarios. Más adelante se iría revelando que esta colaboración había sido una constante entre algunas empresas del sector tecnológico. Las sospechas de la existencia de "puertas traseras" en los sistemas operativos

---

534 AA.VV. *Echelon. La red de espionaje planetario*. Melusina. Barcelona. 2007

535 . Echelon no ha dejado de estar en funcionamiento desde los inicios de la guerra fría. En este sentido, publicaciones tan recientes como la crónica de Duncan Campbell, *The GCHQ and me. My life unmasking British Eavesdroppes*, publicada en The Intercept el 3 de agosto de 2015, actualizan la información disponible públicamente sobre esta red global de espionaje electrónico.
Disponible en: https://firstlook.org/theintercept/2015/08/03/life-unmasking-british-eavesdroppers/ . Por seguridad, al tratarse de una fuente de especial interés, mantengo una copia en: http://www.evernote.com/l/ACuvHl9iXVdDobouCB-WSoHxNKuaez4lOig/

que permitían un acceso a los datos del usuario no reconocidas públicamente se irían confirmando[536].Por una filtración sabríamos por ejemplo cómo Microsoft suministró a las agencias policiales y de seguridad de su país una herramienta denominada *Microsoft Cofee*, que permitía hacer reportes forenses completos de las maquinas con su sistema operativo. Probando la herramienta filtrada, todavía hoy es capaz de extraer datos sustanciales sin muchos conocimientos, o la introducción de software espía en máquinas para controlar el tráfico y acceder a sus archivos de forma indetectable[537]. Otros casos como Twitter, nos demostraron una tensión permanente entre la salvaguarda de los datos de sus usuarios y las presiones por parte de los organismos de seguridad de EEUU. Así, sabríamos que finalmente, con diferentes reparos por parte de algunas, la mayoría de las empresas tecnológicas y de internet con sede en EEUU terminarán prestando soporte a sus organismos de seguridad.

No solo organizaciones sociales sino el mundo del *hacking*, agrupados bajo la identidad genérica de *Anonymous* (surgida del foro anónimo de *4Chan*, sobre todo en su *lista /b* o "random"), iniciarían una serie de ataques de denegación de servicio (DDoS) contra las principales empresas que negaban servicios a WikiLeaks[538]. Así Visa, MasterCard o

---

[536] Entre las reflexiones a propósito del nuevo escenario surgido a raíz de las revelaciones de la gran estructura de vigilancia cuidadana indiscriminada compondría un artículo sobre sus consecuencias titulado *El fin de la inocencia en la red:,* disponible en http://www.eldiario.es/turing/inocencia-red-internet_0_146635468.html y en http://www.rebelion.org/noticia.php?id=170310

[537] El software espía Spyfiles, es un malware que se integra y oculta en el sistema operativo de la víctima para acceder a sus datos privados de forma oculta: https://wikileaks.org/the-spyfiles.html

[538] La denominada Operación Playback (venganza), se haría empleando el ya tratado LOIC, una herramienta para realizar ataques de denegación de servicio capaz de bloquear sitios web. Con la incorporación del modo "Hive Mind", se pudo controlar las maquinas atacantes desde un canal de chat IRC. Con ello se conseguiría un aluvión de ataques de diversas procedencias capaz de tumbar webs que en aquellos momentos no estaban preparadas para mitigar este tipo de atraques. *The Guardian* recogería información interesante del asunto: http://www.theguardian.com/media/2010/dec/08/operation-

PayPal, sufrirán no solo la campaña en la red de estos hactivistas sino una campaña de boicot por parte del activismo cívico, condenando la actitud servil a los intereses del espionaje norteamericano y una puesta en cuestión de los sistemas de pago electrónicos más extendidos en la actualidad, radicados también en territorio estadounidense.

Los ataques DDoS ya había sido un método para tratar de censurar la propia página de WikiLeaks. La migración de las bases de datos a los potentes servidores de *Amazon EC2* sería una solución temporal con escaso recorrido, ya que la empresa decidió rescindir el contrato con la Wiki de filtraciones igual que la francesa OVH, a instancias del ministro francés Eric Besson. Como reacción a este intento de silenciar a la página, multitud de colectivos y simpatizantes empiezan a levantar espejos (copias completas de la página) en diversos servidores propios a lo largo de múltiples localizaciones. En poco tiempo, WikiLeaks se ve sometido a un bloqueo y ataque por múltiples frentes, desde Internet, los gobiernos y las entidades financieras [539] . Por suerte, al intento de asfixia financiera responde la islandesa *DataCell*, que trata de canalizar las donaciones de nuevo hacia el portal. La negativa de Visa, MasterCard, American Express y PayPal a permitir transferencias hacia la cuenta de WikiLeaks provocará que los islandeses denuncien a las entidades internacionales, lo que desembocará en la condena por parte del tribunal supremo Islandés[540], a Visa en primer lugar, con una sanción económica de 6.830€ por día de retraso en la obligación de restaurar los métodos de pago a la

payback-mastercard-website-wikileaks

[539] Dans,E*: WikiLeaks gana, Visa pierde* en: http://www.enriquedans.com/2013/04/wikileaks-gana-visa-pierde.html

[540] La nota de prensa en la que Julian Assange confirma la condena del tribunal supremo islandés a Visa por bloquear las cuentas y las formas de pago a WikiLeaks: http://www.twitlonger.com/show/n_1rjulqn

organización[541]. De este modo y gracias a mecanismos alternativos de donación, WikiLeaks conseguirá finalmente sortear el acoso financiero a lo largo de 2012.

Ataque y cárcel para los filtradores

Uno de los primeros perjudicados del escándalo será el soldado Bradley Manning[542], del que se sospechada, como más adelante sería confirmado, que pudo extraer un grueso importante de esa documentación desde un dispositivo de memoria USB [543] . Manning, será la fuente principal de las primeras filtraciones del *cablegate*. La cantidad de información extraída, tras ponerse en contacto con WikiLeaks y exponer que tenía acceso a documentación comprometedora, desde su puesto en Bagdad, conformará la base de la primera oleada de filtraciones de la web. La extracción de toda la información y su publicación por parte de la organización de filtraciones pondría inmediatamente tras su pista al comando de Investigación Criminal del Ejército de los Estados Unidos que precedería a su detención en mayo de 2010. Las condiciones de su encarcelamiento, serán condenadas por Amnistía Internacional o Human Rights Watch. Su juicio, celebrado en mayo de 2013 y su condena a 35 años de prisión es un tema que todavía provoca serios debates entre los

[541] La condena a Visa por el Tribunal supremo de Islandia supondría la primar victoria frente a la ofensiva de varios gobiernos y empresas contra WikiLeaks http://arstechnica.com/tech-policy/2013/04/supreme-court-of-iceland-rules-firm-must-process-donations-for-wikileaks/

[542] La web de solidaridad con el exsoldado preso Bradley Manning (ahora Chelsea Manning), mantiene información actualizada sobre su situación: http://www.chelseamanning.org/

[543] Sobre las primeras informaciones de Bradley Manning http://www.genbeta.com/activismo-online/una-web-y-un-soldado

defensores de derechos humanos. Ahora mismo, Chelsea Manning, que adoptaría su nueva identidad de género tras el juicio, dado que previamente no había reconocimiento militar a la posibilidad de tal cambio, pretende afrontar una apelación para la que existe incluso una campaña de crowfounding, impulsada por la publicación *The Intercepter*, para el año 2015[544].

La principal figura de la asociación, su fundador, Julian Assange, será también víctima de un rocambolesco proceso judicial a nivel internacional. La idea del gobierno estadounidense, partía de acusar a Assange y a tantos miembros de WikiLeaks como pudiera de traición, al revelar informaciones confidenciales. En lo que respecta al Propio Assange, el proceso de extradición entre Gran Bretaña y Suecia por el extraño caso en torno a un delito de agresión sexual, por un segundo contacto sexual no consentido causa extrañeza entre los que tratan de conocerlo en detalle. Más allá de valoraciones, el delito, solo tipificado en Suecia, significa que hay una orden de extradición contra Assange, que sería detenido y puesto en libertad, para volver a ser buscado por una orden internacional de captura emitida desde Suecia. Finalmente, en junio de 2012, se refugiaría en la embajada de Ecuador en Londres, donde permanece como refugiado desde entonces. A pesar de tener concedido asilo en Ecuador, se encuentra confinado en la embajada, dado que tiene la certeza que de salir sería detenido. El temor real es que tras toda esta tramoya legal se oculte una extradición forzosa a EEUU donde se le podría

[544] La campaña de *CrownFounding* para la apelación al juicio de Chelsea Manning impulsada a lo largo del veranos de 2015 por The Intercept, pretende volver a valorar el tipo de información suministrada por la ex soldado : http://www.chelseamanning.org/news/new-crowd-funding-campaign-for-chelseas-legal-fees-launched-by-freedom-of-the-press-foundation

acusar de revelación de secretos acogiéndose a la legislación más reciente y enfrentarse incluso a una eventual condena a muerte[545].

Todo esto llevaría a WikiLeaks y a su fundador, en una simbiosis indisoluble, a convertirse en auténticos fenómenos populares, en palabras de Daniel Domscheit-Berg. También sería el inicio de una crítica interna tanto por el personalismo adoptado por su fundador como por la no completa garantía de anonimato de las fuentes. Ello llevará a que varios miembros como El propio Domscheit, abandone el proyecto para lanzar otro de similares características, como el denominado *Openleaks*[546]. Otros colaboradores, también han pasado a reforzar proyectos ya existentes como Cryptome, que hoy en día sigue siendo una de las principales plataformas de filtrado de información confidencial[547].

Por su parte, desde WikiLeaks se daría un paso sobre el que se ha especulado mucho desde el momento, con la publicación de un archivo cifrado (con una llave criptográfica AES de 256 bits) [548] denominado

---

[545] Assange, J. *Cypherpunks. La libertad y el futuro de internet*. Deusto. Madrid. 2014

[546] Dromscheit-Berg, D. *Dentro de WikiLeaks. Mi etapa en la web más peligrosa del mundo*. Roca. Barcelona. 2011

[547] Cryptome es para muchos la página que continúa el testigo de WikiLeaks en cuento a revelaciones de secretos y publicación de archivos. La página es incluso anterior a esta primera, aunque sea menos conocida. En la actualidad, es una de las fuentes más fiables para el periodismo de investigación sobre informaciones concretas acerca del espionaje de EEUU: http://www.cryptome.org/

[548] Las claves de cifrados, como la AES de 256 bits de este caso, significa que los ficheros están codificados con un protocolo de seguridad específico que solo puede ser descifrado mediante una contraseña especial, llamada Llave Criptográfica, de lo contrario no hay forma de ver el fichero. A día de hoy, esta clave es suficientemente robusta para aguantar intentos de descifrados con las técnicas más usuales (diccionarios o fuerza bruta).

29. Algunos sitios que contiene el archivo *insurance.aes256:*

insurance.aes256, con un tamaño de 1,39 Gb, mediante su difusión por redes *torrent* y que todavía está disponible en bases de datos (trackers de torrents) y diferentes sitios de descargas. Con ese nombre, se puede pensar que se trata de un paquete de información especialmente comprometida, dado que su difusión se hace con el condicional de que en caso de que a los miembros de WikiLeaks les sucediera algo se revelaría la clave para su descifrado, a modo de plan de contingencia[549]. Mucho se ha especulado al respecto al carácter del contenido del archivo y de por

---

HTTP (en descarga directa)

http://dump.udderweb.com/Censorship/insurance.aes256

http://files.openduck.com/mirror/insurance.aes256

http://insurance.aes256.org/insurance.aes256

http://klockenstein.se/temp/WikiLeaks/insurance.aes256

http://media.kane.cx/~kane/insurance.aes256

http://mirror.openstreetmap.nl/wikileaks/insurance.aes256

http://mrkva.eu/~mrkva/insurance.aes256

http://repo.life-hack.org/wikileaks_insurance/insurance.aes256

http://wikileaksinsurance.org/insurance.aes256

http://wired.s6n.com/leakswiki/insurance.aes256

Torrent (mediante torrents)

http://isohunt.com/download/202524325/76a36f1d11c72eb5663eeb4cf31e351321efa3a3.torrent

http://torcache.net/torrent/76A36F1D11C72EB5663EEB4CF31E351321EFA3A3.torrent

http://torrents.thepiratebay.org/5723136/WikiLeaks_insurance.5723136.TPB.torrent

http://torrage.com/torrent/76A36F1D11C72EB5663EEB4CF31E351321EFA3A3.torrent

[549] Ni siquiera el propio Assange, es sus diversas entrevistas ni sus libros y colaboracionesmas recientes ha querido desvelr el contenido del archivo cifrado mas allá del porósito con el que defiende su existencia. Así, a pesar de las múltiples ideas en torno a este, lo mas probable sea que se traten de archivos especialmente compormetidos, incluso en un sentido vinculado a aspectos relacionados con la seguirdad, y que por tanto se haya preferido que formen parte de dicho "pan de contengencia" antes que ser revelados.

qué no se ha incorporado la información a las filtraciones ya vertidas. Lo cierto es que el caso de WikiLeaks, que se ha convertido en una plataforma de filtraciones mediante la que poder llevar informaciones con la garantía de preservar la fuente, se ha convertido en una nueva forma de conocer cómo medios y gobiernos juegan una serie de intereses que no se corresponden con el global de la población.

El precedente de WikiLeaks, ha inspirado múltiples plataformas para gestionar informaciones confidenciales o comprometedoras. Incluso surgirían aplicaciones como *whisper*, para comentar dentro de círculos concretos información acerca de su entorno. Otras plataformas internacionales con un carácter más exclusivamente periodístico y con garantías para la fuentes podrían ser la Asociación internacional Whisteblowing Press, que ha tenido un papel importante en la revelación de negociaciones secretas entre la UE y EEUU[550]. En España, donde los escándalos de corrupción se han multiplicado tras el estallido de la crisis y la burbuja inmobiliaria, también han surgido plataformas de especial interés en lo que respecta a la denuncia de corrupción principalmente. Así plataformas como Fíltrala, permiten gestionar informaciones manteniendo la confidencialidad de quien la suministra. La colaboración de medios periodísticos no identificados con los poderes del sistema bipartidista, ha permitido dar a conocer casos de corrupción de primer nivel y ha permitido la puesta en circulación de informaciones que de otro modo no habrían salido a la luz. Nuevos medios de comunicación nacidos en la red con un enfoque periodístico más libre de influencias como *Diagonal* , *El Diario,*

[550] Asociación internacional Whisteblowing Press. Una asociación que pretende garantizar la confidencialidad de las fuentes y la colaboración de medios independientes en su análisis y publicación. ,https://awp.is/

La Marea y Mongolia (este último de corte satírico) colaboraran con esta plataforma en el procesado y publicación de informaciones[551].

Especial importancia han tenido las filtraciones respecto a las negociaciones del TTIP, que se plantean en unos términos parecidos al ACTA, como ya hemos visto en capítulos anteriores. La clave de todo el asunto vuelve a estar en la puesta en conocimiento público de las motivaciones reales de los acuerdos, como ya ocurriera en la anterior ocasión y que dejaba en mal lugar a los integrantes de los comités negociadores.

El caso Snowden

Aunque no ha sido el último y no es intención nuestra hacer una crónica exhaustiva de los sucesivos escándalos a consecuencia de las más recientes revelaciones, el caso en particular de Edward Snowden merece un apartado propio por la singularidad de su situación, tanto por ser personal interno dedicado a una de las contratas en las que las diversas agencias de seguridad norteamericanas delegan para los aspectos más particulares del espionaje vinculado a las diferentes formas de comunicación a través de la red como por loa trascendencia del material filtrado. Como empleado de la CIA y la NSA y posteriormente como especialista e una consultora de la NSA, Snowden sería capaz de hacerse con información de primer orden acerca de los mecanismos de espionaje

[551] La plataforma española de revelación y denuncia Fítrala, está destacando en las cuestiones de corrupción y las negociaciones secretas de tratados internacionales. Medios independientes españoles colaboran en el análisis y publicación de la documentación suministrada. Los medios son Diagonal (https://www.diagonalperiodico.net/), El Diario (http://www.eldiario.es).es, La Marea (http://www.lamarea.com) y Mongolia (http://www.revistamongolia.com/). La página del proyecto es: https://filtrala.org/

más sofisticados que las inteligencias estadounidenses y británicas estaban empleando y poniendo en práctica[552].

Snowden, afincado entonces en Hawái, huiría el primero de mayo de 2013 a Hong Kong y desde una habitación de hotel, suministraría a los diarios *The Guardian* y *The Washington Post la* información recogida durante su periodo como consultor dentro de la organización de inteligencia estadounidense. Una vez revelada su identidad, cursaría una serie de peticiones de asilo, ante el temor por su seguridad. La presión, estadounidense, que anularía su pasaporte, le hará tomar un vuelo a Moscú y solicitar asilo en Ecuador. El 3 de julio de 2013, la negativa de, Francia, Portugal, Italia y España, de permitir escala en sus respectivos territorios del avión diplomático del presidente de Bolivia, Evo Morales, proveniente de Moscú ante las sospechas de que en el avión podía ir el propio Snowden, provocaría un conflicto diplomático y dejará claro al confidente que no era seguro un eventual vuelo hacia Ecuador. Así, el peligro de ser interceptado inmovilizaría a Snowden en la capital rusa, país que no tiene acuerdo de extradición con EEUU y en el que desde entonces reside[553].

Los famosos *papeles* de Snowden recogidos y publicados por el entonces periodista de *The Guardian*, Alan Greenwald, tendrán por si

---

[552] *CitizenFour*. El galardonado documental, dirigido por Laura Poitras, sobre el caso de Edward Snowden y las consecuencias de las revelaciones de este: https://citizenfourfilm.com/

[553] Los artículos del diario *The Guardian* en torno a la NSA y que tanta polémica desataron se encuentran bajo la etiqueta siguiente: http://www.theguardian.com/us-news/the-nsa-files

mismos un relato propio del más genuino estilo de espionaje. La reacción de GCHQ, con la retención de la pareja de Greenwald, de nacionalidad brasileña, en una escala en Heathrow tras viajar este a Berlín a entrevistarse con Laura Poitras, otra documentalista estadounidense que también analizaba la información proporcionada por Snowden y la posterior incautación de terminales y discos duros, e incluso el capítulo de destrucción de discos duros en el sótano de la redacción del diario supondrá un relato de hasta qué extremo se había llegado en la intención de ocultar lo que todo el conjunto documental extraído por Snowden. En ese sentido, la puesta a disposición del conjunto de instrumentos de espionaje de la NSA y sus aliados, juntos con los informes de espionaje a naciones y líderes aliados, descritos con todo detalle, dejará en una posición comprometida a los gobiernos estadounidense y británico, colaborador este último en buena parte del trasfondo europeo[554] de todo el escándalo.

El propio relato de Greenwald, que finalmente optaría por mantener su actividad periodística desde Brasil, país que no mantiene acuerdo de extradición ni con EEUU ni con Gran Bretaña, nos demuestra hasta qué extremo se llegaría por parte de los gobiernos afectados por la ocultación de las pruebas de unos métodos de espionaje poco claros. Finalmente, el periodista dejará el diario, sometido por su parte a constantes presiones no siempre reveladas, para que no publicara más datos. Con ello, el medio en si perderá buena parte de su credibilidad, al interpretarse tal abandono como una cesión a intereses británicos y abundará en la importancia de medios independientes.

[554] Greenwald, Glenn - Snowden. Sin un lugar donde esconderse. Ediciones B. Barcelona. 2014

Como hemos descrito en el capítulo anterior, buena parte de los métodos modernos de espionaje en la red serán revelados por Snowden o dejará confirmada su existencia. PRISM o XKeyscore serán programas cuya existencia no se conocía hasta el momento y que dan cuenta del alcance que el espionaje electrónico ha llegado a alcanzar en nuestros tiempos [555]. La completa exposición a los metidos de espionaje del conjunto de la ciudadanía será así confirmada por una fuente de primer orden, con profusión de datos detallados. La dimensión de toda la información puesta en conocimiento público ha significado una pérdida de confianza por parte de la ciudadanía más activa y del mismo periodismo de investigación hacia los gobiernos, que han alimentado una maquinaria, en buena medida mediante contratas privadas, para someter a un espionaje arbitrario de injustificado a todo el conjunto de la población de sus respectivos países[556].

La NSA y el GCHQ británico llegarían a manipular la fabricación de tarjetas SIM del principal fabricante mundial, *Gemalto*, para acceder a las ubicaciones y emisiones de los teléfonos móviles desde origen. Pudiendo descifrar los contenidos que circulan como las llamadas o los SMS[557]. Asimismo se sabrá de la manipulación por parte de la NSA de aparatos de infraestructura de red, como los Routers, para mantener

---

[555] Banford, J. *The Most wanted man in the world*. Wired. 2014. Recurso disponible en: http://www.wired.com/2014/08/edward-snowden/#ch-1

[556] Privacy Internacional y Amnistía internacional han publicado un informe sobre el estado de la cuestión de las revelaciones de Edward Snowden titulado "*Two Years after Snowden. Protecting Human Rights in an age of mass surveillance"*. Disponible en: https://www.privacyinternational.org/?q=node/591

[557] Snowden también revelaría cómo el mayor fabricante de tarjetas SIM del mundo y por tanto la de la mayor parte de las que se encuentran en nuestros terminales, será *hackeada* por la NSA introduciendo código capaz de rastrearnos:http://www.theguardian.com/commentisfree/2015/mar/08/edward-snowden-trust-phone-laptop-sim-cards

abiertas vías de espionaje a través de estos dispositivos y poder infiltrarse en las redes personales. El montante total de la campaña para influir en los diseños tecnológicos de las grandes de Silicon Valley llegaría a los 250 millones de dólares. Curiosamente, al tiempo que se desataba una polémica sobre los dispositivos de acceso de fabricantes Chinos como Huawei, no afectados por tal caso, bajo la sospecha de que China podía estar dejando "puertas traseras" en los dispositivos de la marca. La cascada de revelaciones suscitará un debate público que por primera vez superará la doctrina de la seguridad para volver a situar la privacidad en el centro del debate. Esto llegará hasta el extremo de la revisión, en muchos aspectos estética, por parte del gobierno de los EEUU de la legislación sobre la vigilancia, algo que no ha supuesto la suspensión de ninguno de los programas descritos.

Como vimos, tras las sospechas suscitadas por WikiLeaks, las compañías Facebook, Google, Apple, Twitter o Microsoft, entre otras, elevarían una campaña para la reforma de la vigilancia gubernamental, y que se suspenda la captación masiva de datos personales de la ciudadanía[558]. La campaña surgirá de forma paralela a las revelaciones sobre cómo la NSA no solo presionaba sino que pagaba a las grandes compañías de internet para que permitir que el sistema PRISM siguiera penetrando servidores de comunicación de empresas como Google, Yahoo! Microsoft y Facebook, merced a la legislación de FISA (*Foreign Intelligence Surveillance Act*) que obligaba al gobierno a devolver los supuestos costes a estas compañías de la implantación y uso del citado sistema de espionaje[559].

[558] La campaña de las grandes compañías de internet norteamericanas en favor de la reforma de la legislación sobre la vigilancia: https://www.reformgovernmentsurveillance.com/

[559] Finalmente se sabría que la NSA no solo presionaba si no que pagaba a grandes

La sociedad norteamericana, foco de buena parte de estas revelaciones se mostrara inquieta ante la dimensión del espionaje y la vulneración permanente de su intimidad[560]. El papel tan discutido de las empresas norteamericanas estaba empezando a calar entre el público internacional y la desconfianza en servicios en la nube de sitios radicados en EEUU podía terminar significando una pérdida de cuota de mercado y la potenciación de alternativas. En pleno proceso de expansión de la nube y las tecnologías móviles, una oleada de sospecha comenzaría a extenderse entre estos servicios. Pero como veremos, la reacción de mayor calado será la de la comunidad hacker y el activismo en la red, que acudirán a medios de cifrado y la investigación de métodos seguros de comunicación que imposibiliten o dificulten la vigilancia, como veremos en siguientes capítulos[561]. Las legislaciones restrictivas y penalizadoras del copyright ya habían potenciado el uso extensivo de elementos de este tipo. Ahora, el espionaje masivo, completará el itinerario y lo elevará a empresas y organismos públicos.

En el resto del mundo, Amnistía internacional lideraría una campaña en contra de la vigilancia[562]. La encuesta publicada al respecto, revela la

---

empresas para que ofrecieran datos de sus usuarios como se filtrará en The Guardian en agosto de 2013: http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid

[560] Encuesta sobre la percepción de la seguridad y la privacidad del Pew Research Center. Disponible en: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/#

[561] En ocasiones, la Wikipedia puede legar a ser una de las fuentes de primer orden dado que la permanencia de sus publicaciones no están sujetas a redacciones de periódicos. Tal es el caso del artículo que hace detallado recuento de programas de espionaje masivo revelados desde 2013 a 2015: https://es.wikipedia.org/wiki/Revelaciones_sobre_la_red_de_vigilancia_mundial_%28201 3-2015%29

[562] La campaña *Dejen de seguirme*, incluye una encuesta y una justificación que terminaría en una demanda contra la

preocupación creciente de la población en torno al asunto y justificaría la demanda interpuesta por la ONG contra la NSA, al no existir justificación legal para un uso extensivo de la vigilancia a toda la población ni la fiscalización permanente de las comunicaciones sin orden judicial[563].

Más filtradores contra la opacidad política y económica

Como hemos visto, la última década del presente siglo, ha supuesto u vuelco completo en lo que respecta a la capacidad de transparentar secretos de estado y acciones poco ejemplares de la mayor parte de los gobiernos. Espionaje y corrupción, han sido los dos grandes temas que han salido a superficie mediante sucesivas revelaciones, la mayor parte proveniente de personas que han tenido acceso a una información de primer orden y cuya responsabilidad cívica les ha impedido mantenerla oculta. Desgraciadamente, la mayor parte de estos ha sufrido la persecución y el acoso, junto con el reconocimiento internacional de organizaciones de derecho. Entre los casos más destacados de esta última década, pocos son los que no han pasado por prisión o se encuentran huídos o en situación asilo. En España, el caso de Hervé Falciani resulta paradigmático[564].

NSA: https://www.es.amnesty.org/dejendeseguirme/encuesta

563 El blog en español de Amnistía Internacional, explica los motivos de la demanda a la NSA: http://www.eldiario.es/amnistiaespana/demandado-NSA_6_367873228.html

564 Sobre Hervé Falciani y el llamado *Swissleaks* existe una espléndida recolocación de material en la publicación española *La Marea*: http://www.lamarea.com/el-swissleaks-de-falciani/

El reconocimiento de la existencia de cuentas opacas en paraísos fiscales, al amparo de autoridades de estas naciones o enclaves, es una de esas situaciones que revela claramente cómo la corrupción y la ocultación de bienes son una constante entre adinerados de todo el mundo. Suiza, por ser un enclave estratégico en Europa y su larga trayectoria en la acogida de maletines y de un turismo selecto entre los más granado del continente, siempre ha sido ejemplo de lo que el secreto bancario significa realmente. El informativo Falciani, se pudo hacer en el transcurso de su actividad profesional en el banco Suizo HSBC (filial del británico del mismo nombre) con una cantidad de datos que rondan los 100 Gb de información. El montante de estos datos pondrían en compromiso a la mayor parte de los depositarios de cuentas secretas, dado que se había conseguido encontrar una vulnerabilidad en el sistema que le permite vincular cuentas y nombres y por tanto conocer los depósitos personales de 127.000 registros de evasores fiscales de buena parte del mundo. El papel de la banca privada en la gestión de cuentas opacas, evasión fiscal y lavado de dinero, impulsaría a Falciani a abandonar Suiza y denunciar antes las autoridades de varios países la existencia de estos datos. En primer lugar pasaría por Francia, en 2009. Finalmente, terminará en España, donde pasaría unos meses en prisión preventiva ante la denuncia de Suiza, por revelación de secretos, hasta que la Audiencia Nacional decretó su libertad condicional y la no extradición. Su colaboración con la justicia francesa y española, llevaría a la revelación de grandes fortunas vinculadas a nombres como los Botín o lo Pujol, en nuestro país o pistas esenciales para hacer un seguimiento más precisos de tramas corruptas como la llamada *Gürtel*, de destacados miembros del PP[565].

[565] ¿Quién es Falciani? ¿Qué sabe Falciani? Un reportaje en el diario, que explica las claves del asunto: http://www.eldiario.es/economia/falciani-HSBC-quien_0_80842176.html

Otros ejemplos han sido aún más contraproducentes para el filtrador en cuestión. El caso de Barret Brown, un periodista muy relacionado con activistas de internet y concretamente con varias acciones de Anonymous, de cuyos ataques pudo extraer información que revelaría la trama de contratas militares alrededor del Departamento de Defensa estadounidense. En este sentido, se convertiría en la fuente de publicación de la situación de las más de 2.000 contratas vinculadas a la seguridad privada y el espionaje que mantiene el gobierno de EEUU. La revelación de la actividad de ciertas compañías privadas, vinculadas a ex agentes de la CIA, como *Abraxas* o *HB Gary*, *hackeada* por Anonymous, expondrían a Brown al ataque de estas empresas. Este *hackeo*, junto con el del grupo *Themis*, otra contrata de seguridad, que pretendían infiltrarse en grupos de Anonymous, pondría en manos de Brown información de primer orden sobre las cuantías y naturaleza de algunas contratas, como el programa denominado *Palantir*, que se dedicaría a la minería de datos personales[566]. La importancia de los datos y la vinculación de miembros de la defensa con un sector privado en busca de contratas millonarias, colocarán a Brown como una figura incómoda y movilizará un itinerario de persecución ya conocido. En marzo de 2012, se registra su domicilio, a lo que el periodista cometería el error de responder con un vídeo en YouTube. En septiembre será detenido sin cargos en primera instancia. El sumario que se irá creando sobre la marcha para incriminarle y será el resultado de compendio de enlaces y comentarios de Brown en medios como Twitter y YouTube, mediante el que se trata de hacer de este un miembro del grupo

[566] Sobre el asunto de las contratas privadas Barret Brown, publicaría bastante información extraída de fuentes cercanas a Anonymous. Existe poca información al respecto en castellano. En 2013 compuse un artículo previo a su definitiva acusación: Quién es Barrett Brown, el periodista especializado en espionaje que está en la cárcel: http://www.eldiario.es/turing/privatizacion-espionaje-periodista-Barret-Brown_0_150485289.html

Anonymous, para incriminarle de delitos de espionaje, o revelación de información privada. Algo complejo para quien no tiene mayores conocimientos que los de un usuario medio dedicado al periodismo. Lo más destacado del caso, es que al tener menor repercusión, apenas es conocido por medios fuera de EEUU, a pesar de tratarse de otro caso de periodista encarcelado por filtrar o publicar sobre tramas de espionaje[567]. Actualmente, existe una campaña para dar a conocer su caso y apelar un juicio que mantiene muchas sombras sobre cómo se ha orquestado y que mantiene silenciado un importante caso de denuncia periodística[568].

Los casos en torno a activistas perseguidos no serán extraños en EEUU, al calor de la *Patriot Act* y el ambiente entre las agencias implicadas tras el aluvión de filtraciones, muy cuestionadas a lo largo de la última década, los métodos frente al activismo llegarían a endurecerse. El ejemplo de Aaron Swartz, será uno de los más reconocidos, al ser uno de los socios más destacados de la EFF y creador del famoso *RSS* (la forma de acceder a nuevos contenidos de una web de forma externa) y de buena parte del código de *Reddit*, una de las redes similares a un foro más famosas de EEUU. Lo desgraciado del caso, que terminaría con su suicidio, atraería aún más, si cabe, la atención de los medios. En esta ocasión se tratará de un activista que trataría de liberar contenidos académicos del MIT, lo que derivaría en una denuncia. Lo más

---

[567] Actualmente contamos con dos documentales que relatan el caso de Brown: S*omos Legión La Historia de los Hactivistas*: https://www.youtube.com/watch?v=ee19z6D1yxo. Su web oficial: http://wearelegionthedocumentary.com/ y el reciente, *The hackers wars.* Un documental sobre los ataques de Anonymous y otros grupos: https://www.youtube.com/watch?t=221&v=YxFH4uJ9qXE

[568] Sobre la detención de Barret Brown, existe una campaña abierta por su liberación: https://freebarrettbrown.org/

destacado de un asunto, sin gran recorrido por sí mismo, será la dureza de su persecución que marcará un precedente para la comunidad hacker y activista. El caso en cuestión, se convertiría en una ocasión para atacar a uno de los representantes más destacados de la EFF por parte del FBI, tantas veces acusado por esta organización de abusos. El especial empeño inquisitivo de los agentes dejaría un halo de sospecha poco claro respecto a todo el asunto, tanto por su dramático final como por lo insignificante de la cuestión legal finalmente esgrimida[569].

Como apunte final, también en Europa la persecución al activismo sigue siendo noticia. El caso de los dos periodistas alemanes del blog *Netpolik*, acusados por la autoridades del país de traición y revelación de secretos ha pasado al primer plano informativo en un país que tiene una especial sensibilidad en cuanto a la persecución del activismo político[570]. Un caso que se ha revelado en agosto de 2015 y que tiene unas connotaciones oscuras. André Meister y Markus Beckedahl, publicarían en su web que el servicio de inteligencia alemán planeaba ampliar sus sistemas de vigilancia electrónica con la excusa del terrorismo. Así la publicación de documentos confidenciales a propósito de asunto, que llegaron a manos de los periodistas hace que ahora mismo se enfrenten una acusación por traición[571]. El caso vuelve a abrir el debate sobre

---

[569] En su momento seguiría el caso De Aaron Swartz, que obtuvo gran transcendencia en ciertos círculos de internet y generaría un movimiento de indignación contra el FBI: ¿Por qué acabar con Aaron Swartz?: http://www.genbeta.com/activismo-online/por-que-acabar-con-aaron-swartz

[570] El blog de los periodistas Netzpolitik (en alemán): https://netzpolitik.org/

[571] El último caso en Alemania en el que acusan a dos periodistas de traición por revelar espionaje estatal: http://www.bbc.com/mundo/noticias/2015/08/150806_libertad_de_expresion_alemania_lb

la divisoria de la libertad de prensa y la naturaleza de los documentos revelados, máxime cuando estos son tan cuestionables como los servicios de espionaje en internet fuera del cauce legal.

La lección de las filtraciones es que si bien han sido la avanzadilla de la madurez ciudadana y una auténtica revelación de la realidad del trasfondos que hay en la red, en la que gobiernos, empresas y delincuentes se han implantado con fuerza, para los que toman el paso ético de hacer público estos contenidos, se les impone un duro futuro.

4.3 Netwar, Cyberwar y hacking dirigido .Terrorismo global en tiempo de comunicaciones inmediatas

La cuestión de la guerra en la red es un tema ampliamente narrado. Este conflicto a escala global abarca a la red al completo y sus objetivos son tan diversos que en nuestra catalogación hemos separado sus orígenes para analizarlos con detenimiento. Así la sustracción de datos sensibles o de carácter personal, el ataque a sistemas industriales, militares o empresariales en general, incluyendo infraestructuras críticas es parte cotidiana de un conflicto en el que llevamos más de dos décadas inmersas aunque la mayor parte de sus consecuencias comiencen a superficiarse en nuestros días.

Podemos localizar tres fuentes distintas de conflicto, cuyos intereses se entrelazan. En una primera instancia, estados enemigos no solo se espían sino que buscan la manera de sabotear infraestructuras básicas del contrincante. En este contexto tecnológico, *ciberguerra* y *cibercrimen* son tan difíciles de separar como complicado dilucidar la diferencia real entre ambos. El tablero geopolítico cuenta con una nueva estrategia en la actores diferentes juegan su influencia de modos muy diversos. En este conflicto, naciones como EEUU, China, Corea del Norte o Rusia, mantienen un papel muy activo y con el tiempo se ha ido filtrando las correspondientes formaciones de divisiones informáticas de sus respectivos ejércitos. Esta fuerza armada Hacker ha sido, de forma escasas veces declarada, protagonista de muchos acontecimientos que en su momento encontraron poca explicación. Así ataques a grandes empresas, virus en instalaciones nucleares, ataques de denegación de servicio y grandes espionajes industriales provendrán en última instancia de una cadena de mando,

incluso en ocasiones donde supuestos hackers autónomos se atribuyan la acción[572].

En el otro extremo, agentes terroristas, que actúan mediante redes internacionales y dentro de los estados en forma de células para evitar la extensión de las detenciones en caso de contingencia. En este aspecto, la propaganda, la infiltración y el sabotaje forman una pauta común entre diferentes grupos terroristas. En los tiempos más recientes, grupos identificados con AlQaeda o con el ISIS (estado islámico de Irak y Siria) aprovechando los ingresos y la extensión de sus redes, han enfocado en la red una serie de campañas y han procedido a la explotación de vulnerabilidades de diversos medios para ejercer su propaganda.

Una tercera fuente, como ya podemos adivinar es la de los hackers que prestan su servicio delictivo a al mejor postor. El incremento de la base de usuarios con conocimientos extendidos acerca de seguridad junto con las perspectivas económicas de un negocio que comienza a ser explorado ha permitido, especialmente entre países menos desarrollados, que lo que en principio fuera una cultura hacker termine derivando en delincuencia, aprovechada convenientemente por la mayor parte de los grupos en liza antes descritos. El gran cambio entre el back hacking, los que se dedican a la delincuencia, ha sido que el motor de sus ataques ha pasado de ser un pasatiempo, o la búsqueda de notoriedad, a perseguir una finalidad económica.

---

[572] Arquilla. J y Ronfeld D. *Network and Netwars. The Future of Terror, Crime and Militancy.* Rand. Santa Mónica. 2014

Los ciberataques con finalidad económica ya sea mediante extorsión, venta de información o por la propia competencia de empresas afectadas, recurren cada vez con mayor asiduidad al mercado negro de la ciberdelincuencia para asegurarse resultados y privacidad. La conocida como *Dark Web*, una parte de la red a la que hay que acceder con ciertos conocimientos y mediante protocolos específicos, mantiene sitios en los que poder hacerse con vulnerabilidades todavía no conocidas, a las que se denomina Zero Day, o alquilar ataques con diversas características. Lo destacable de este cambio es la puesta en servicio de todo un contingente de individuos dispuestos a realizar ataques de diversa índole por motivos económicos y la cantidad de medios que son movilizados para ello[573].

La red se ha convertido en un nuevo centro de poder global. Su capacidad comunicativa y su potencial como instrumento de expansión. Como ya hemos visto, la red ha sido utilizada incluso para captar soldados mediante videojuegos de simulación de guerra, caso del Americas Army[574], videojuego online de corte realista (sus responsables actualizan anualmente el armamento real) mediante el cual el ejército de EEUU trata de captar jóvenes para que se alisten al tiempo que plantean situaciones muy verosímiles para los ya alistados, a modo de entrenamiento virtual. La confluencia de varios elementos en torno al despliegue de recursos empelados como arma seguirá un proceso creciente en torno a la red, máxime cuando la importancia de esta y la multitud de servicios que

---

573 González Pérez, P. *Ethical Hacking*.0xWorld, Madrid. 2014

574 *Americas Army*. El videojuego diseñado para reclutar soldados en EEUU. Sigue hoy en día en activo, actualizando armamento e información constantemente: http://www.americasarmy.com/

dependen de un entorno conectado ha crecido exponencialmente hasta el tiempo presente.

En nuestra introducción ya tratamos de la candidez de dibujar la red como la "aldea global", cuando el símil más adecuado habría sido el del Chicago de los años 20', en el que grandes empresas, cibercriminales y estados se disputan un espacio en el que las libertades individuales son las principales perjudicadas. La guerra en la red, se ha convertido en una fuente de preocupación en la que son más las ocasiones en las que la investigación para el asalto supera las barreas de la seguridad. En la DefCom, la conferencia Hacker más famosa que se celebra todos los meses de agosto en las vegas desde 1992, los responsables de la distribución forense Kali Linux, afirmaban que según sus datos, un tercio del tráfico global de Internet lo ocupan los ataques de denegación de servicio (DDoS)[575]. Con ello, ponemos en perspectiva el auténtico arsenal puesto en circulación. Los organismos de ciberseguridad y las empresas dedicadas a la seguridad de empresas y usuarios, nos detallan u panorama en el que la cantidad de ataques dirigidos. Al analizar los orígenes de los ataques encontramos lugares previsibles como China, Rusia, donde existen asimismo grandes colectivos de hackers.

La supremacía tecnológica ya no depende tanto de la inversión en infraestructuras o el poderío militar. Internet ha conseguido democratizar también en su medida la capacidad de intervención para poner en manos de grupos y naciones con menor capacidad económica todo un arsenal de

[575] Según estudio de los desarrolladores de la distribución forense más reconocida, Kali Linux los ataques DDoS suponen 1/3 del tráfico de internet en 2015: *DDoS attacks constituted about 1/3 of all our traffic today, during our Kali 2.0 release*. pic.twitter.com/1dsahyeytR

recursos que, con dedicación suficiente, puede dar producto a una escala impensable hace unos años[576].

La ciberguerra

El primer ataque informático entre estados del que se tiene constancia certera, de otros precedentes no hay claridad, será el de la guerra de Kósovo, en 1999. Como estrategia de defensa, un grupo de 450 informáticos establecerán un ataque a las instalaciones controladas por ordenador de la OTAN, la Casa Blanca e incluso al portaaviones norteamericano Nimitz, aunque no conseguirían ningún objetivo concreto más allá de la intrusión. El caso, por lo desconocido en su momento, conseguiría cierta repercusión entre medios y cornistas del confito, aunque a efectos prácticos no conseguiría mayor alcance que el propagandístico[577].

Pero las fuentes suelen situar como el primer episodio de ciberguerra realmente declarada y dirigida el de China contra Taiwán en 2003. El ataque dañaría cierto número de infraestructuras y tendría un variado arsenal de infecciones informáticas que provocaría un estado de alarma en el país. Las autoridades de Taipéi, lejos de ocultar la situación, pararían a publicar la envergadura del ataque y difundir la dimensión del asunto, que afectaba desde semáforos hasta hospitales pasando por la propia Bolsa, paralizada durante unos días. Aunque el ataque nunca fuera reivindicado, todas las pruebas apuntarían a una de las primeras intervenciones del

---

576 Assange, J. *Cypherpunks. La libertad y el futuro de internet*. Deusto. Madrid. 2014.

577 Caro, Mª José (2013*). Algunas reflexiones sobre la ciberguerra*. En: Documento informativo del Instituto Español de Estudios Estratégicos, 13/2013 de 24 de abril.

incipiente comando cibernético del ejército Chino[578]. Desde entonces han sido recurrentes las denuncias por parte de los sucesivos gobiernos taiwaneses de ataques cibernéticos por parte de China. Eric Smidt, actual cabeza de Google, llegaría a asegurar que China es una de las principales potencias del hacking y que actualmente pueden rondar el 80% de las incidencias al respecto, dejando en al aire cuantas de estas persiguen motivaciones dirigidas[579].

El 27 de abril de 2007, el gobierno estonio retiró una estatua erigida en los tiempos de la dominación soviética en homenaje a los soldados que lucharon contra la invasión alemana en la Segunda Guerra Mundial. A pesar de ello, la estatua en cuestión era vista por muchos estonio como un signo del periodo bajo la sombra del Kremlin que como un homenaje a estos soldados, por lo que finalmente se decidiría su retirada[580]. La protesta de la población de origen ruso, en torno a un 25% de los estonios, derivaría en el primer gran caso de ciberguerra contra un estado[581]. Precisamente

---

[578] La noticia en su momento publicada por *The Iquire*r, que no añade más que lo que el resto de publicaciones haría en el momento, es decir, recoger la acusación del gobierno taiwanés y describir la incidencia del ataque:

http://www.theinquirer.net/inquirer/news/1012617/taiwan-accuses-china-of-waging-cyberwar

[579] La curiosa posición del CEO de Google respecto a los ataques chinos, debemos verla en perspectiva en primer lugar por la propia salida de Google y sus servicios de China y del papel competidor que juegan plataformas locales como *Baidu* desde entonces, así como el desarrollo de aplicaciones similares a las que desarrolla la propia compañía. Todo ello, en su última publicación: http://www.newdigitalage.com/

[580] En el Documental: *Amenaza Cyberhackers informáticos*. Emitido dentro del programa *Informe Semanal*, de RTVE, explica de manera bastante gráfica el caso de Estonia: https://www.youtube.com/watch?v=Z4X80QNOXc0

[581] El ataque, expresado en cifras sobre el caudal de datos empleados, puede consultarse en : http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

Estonia, es un estado que ha tratado de ubicarse pronto en primera línea pro occidente, colocándose en la cabeza europea de la administración electrónica, donde incluso los consejos de ministros intercambian documentación no impresa mediante el uso de redes. Así lo que en principio fuera una protesta por parte de la población rusa en contra de lo que significaría para ellos una ofensa nacional, pronto pasó a ser un ataque a gran escala conocido como *DDoS* (Ataque por denegación de servicios) mediante el cual, se saturan las redes informáticas de un servidor concreto de peticiones de conexión desde un alud de ubicaciones distintas hasta llevar al colapso a los ordenadores víctimas de esta cantidad exorbitada de peticiones. Lo más destacado de este caso es que, a diferencia de otros ataques, muchas veces realizados por hackers concretos descontentos o al servicio de diversos objetivos sobre una víctima concreta, en esta ocasión, el ataque fue realizado a gran escala contra todos los servicios y organismos de todo un estado concreto, hasta llevarlo a su completa desconexión de la red de redes, afectando incluso a las redes de cajeros automáticos y otros servicios públicos, recientemente integrados. Para hacernos una idea de los parámetros de dicho ataque, según declaraciones del propio ministro de defensa estonio, que pediría asistencia a expertos de la OTAN, las peticiones que a lo largo de un día podría recibir la Web principal de la administración del estado, en torno a unas 20.000, se llegaron a producir por segundo[582]. Esta enorme escala de ataque solo puede producirse gracias a la existencia de una multitud de ordenadores denominados zombis, infectados por una intrusión externa capaz de controlarlos remotamente sin que el usuario en cuestión tenga

[582] La estrategia de ciberdefensa pasará al primer plano en Estonia, máxime desde los pasados incidentes de seguridad. La estrategia de ciberseguridad es actualizada anualmente y publicada por su ministerio de defensa. La del año 2015, puede consultarse en: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/public_opinion_and_national_defence_2015_march_0.pdf

conocimiento de ello. Otra denominación muy usual es la de *bot* (derivada del término *Robot* que Asimov acuñara) y su empleo usual, una vez infectado por un troyano, "caballo de Troya" para ser exactos, o programa instalado para el control remoto del ordenador sin el consentimiento del usuario, es el de envío de *spam* (correo basura por el que algunas compañías pagan al hacker en cuestión). Sin embargo, el dueño de la *botnet* (red de ordenadores *zombies*), es poseedor de un potencial aun mayor que el de el correo basura o el de saltar entre terminales para realizar operaciones bancarias ilegales sin poder ser rastreado, ya que puede sincronizar todos estos ordenadores para que operen en conjunto y realizar ataques como el que tratamos como ejemplo. Según el INTECO (Instituto Nacional de Tecnologías de la Comunicación), redenominado en 2015 a INCIBE (Instituto Nacional de Ciberseguridad) en la actualidad podrían haber alrededor de 700.000 ordenadores[583] operando de tal forma, al servicio de un limitado número de hackers.

El ataque masivo a Estonia, que duraría hasta mediados del mes siguiente, supuso el ejemplo más claro de las nuevas formas de plantear una guerra electrónica y como esta, en una sociedad cada vez más dependiente de la tecnología, puede tener consecuencias mayores de las esperadas. También en este caso, Estonia ha pagado las consecuencias de asumir el monopolio de las soluciones únicas de un sistema operativo y de una compañía, Microsoft. Precisamente la no diversificación de servicios ha sido una de las críticas comunes por parte de múltiples técnicos de sistemas, entendiendo como un error, disponer solamente de las soluciones propietarias comercializadas por esta compañía[584]. Los diferentes CERT,

---

[583] El INCIBE (Instituto Nacional de Ciberseguridad), aparte de referente estatal en temas de ciberseguridad, mantiene un Centro de respuesta a incidentes informáticos para PYMES y ciudadanos. : https://www.incibe.es/

[584] CyberInsecurity: The Cost of Monopoly. El peligro para la seguridad del monopolio de

son cada vez más conscientes del peligro de estas organizaciones. De hecho, desde el principio las sospechas han recaído sobre el gobierno ruso en este caso y el departamento específico que la FSB, heredera de la KGB soviética, mantiene[585]. El asalto a sitios en los que puede poner en duda la forma de dirigirse del gobierno ruso se convertiría en un recurso habitual, sin autoría reconocida, pero una metodología constante. Uno de los casos más significativos sería el del ataque masivo denegación de servicio durante el 6 de agosto de 2009 a *Twitter*, *Blogger, YouTube, Livejournal* y *Facebook*[586], ampliamente recogido en todas los servicios de noticias internacionales[587] y que parece que se ha dirigido contra un bloguero concreto, llamado *Cyxymu* que en su bitácora y a través de todos estos servicios, criticaba a Rusia en el aniversario de su ataque a Georgia, sucedido un año antes.

Desde luego, el crimen organizado, como en tantas otras ocasiones, ha sido uno de los sectores que tempranamente ha sabido sacar provecho de la red de redes. El *hactivismo* primero, en el que conocedores de las formas de explorar las debilidades del sistema funcionaban a modo de pasatiempo para, en definitiva, mejorar la seguridad de este ha pasado a actividades de carácter más lucrativo, poniendo sus conocimientos al

---

Microsoft. : http://cryptome.org/cyberinsecurity.htm

585 Acero, F. *Conclusiones al ciberataque a estonia:* http://www.kriptopolis.org/conclusiones-ciberataques-a-estonia

586 Respecto al ataque, se abrirían multitud de especulaciones al respecto, al ser un caso particular, en el que se señalaba la autoría por parte de un individuo: http://www.genbeta.com/web/el-ataque-ddos-a-twitter-facebook-google-livejournal-iba-dirigido-contra-un-solo-hombre

587 El ataque, sería interpretado en ciertos círculos estadounidenses como un reto a su posición respecto a países de la esfera de influencia rusa y por tanto tendría bastante repercusión en los medios. Una selección de noticias en EEUU sobre el ataque masivo está disponible en: http://news.bnonews.com/hs33

servicio de la estafa o el espionaje por Internet. Las propias agencias de espionaje estatales y muchas compañías han sabido fichar o tener cerca a muchos de estos jóvenes, captándolos para sus propios fines. De hecho la misma OTAN acaba de llevar adelante un programa denominado K5 (Centro Cooperativo de Ciberdefensa de Excelencia), mediante el que pretenden defenderse y pasar a una posición activa ante ciberataques como los antes descritos [588]. Curiosamente, la base central de este organismo se ha ubicado a las afueras de Tallin.

La lista de grandes ataques, con mayor o menos fama, son objeto de estudio entre los profesionales de la seguridad. Así nombre como *Flame*, *Duqu* o *Stuxnet* pasarán a la galería de ataques más virulentos en lo que respecta a nuevos métodos de intrusión en sistemas, incluso desconectados de la red global. Las formas en las que el proceso de pruebas de penetración (*pentesting*) y adquisición de conocimientos respecto al objeto a atacar han conseguido desmontar ciertos esquemas de seguridad al tratarse de importantes ataques dirigidos con virus con diseños muy sofisticados enfocados a no ser detectados y extraer el máximo de información de la víctima de forma desatendida y autónoma.

El ataque a las instalaciones nucleares iraníes en 2010, significará otro paso más en dicha estrategia, al conseguir penetrar en sistemas teóricamente aislados mediante la intrusión física de un dispositivo de memoria para propagar después la infección dentro de dichas instalaciones y poder proceder el sabotaje. Detrás de esta intervención estaría desde su origen la sombra de Israel y EEUU. Efectivamente, el análisis posterior de

[588] Sobre el grupo K5, el diario británico The Guardian elaboraría un reportaje extenso: http://www.guardian.co.uk/technology/2009/apr/16/internet-hacking-cyber-war-nato

Stuxnet, no dejaría dudas acerca del origen y objetivo de su programación. Un sistema preparado para dañar las instalaciones industriales diseño de la empresa alemana Siemens, en concreto las centrifugadoras de gas. Posteriormente se filtrara dicha colaboración para el uso de la primera gran ciber-arma diseñada con un objetivo tan concreto[589]. Posteriormente, *Duqu*, seguirá el esquema de arma cibernética para el sabotaje de instalaciones industriales[590]. Otra gran ciber-arma liberada en 2012 tendrá consecuencias todavía mayores, al tener una orientación distinta, *Flame*. Este malware modular, será capaz de adquirir datos de fuentes diversas una vez ubicado en un ordenador, desde pulsaciones de teclado, tráfico de red, capturas de pantallas y en general todos los procesos que se ejecuten en el sistema víctima. Sin querer extendernos en la descripción de sus cualidades, su expansión entre ONG y países como irán, Sudan o Siria, ya nos podría en la pista de su origen[591]. Así lo afirmaría en su momento uno de sus descubridores, el ruso Eugene Kaspersky, dueño de la compañía de seguridad del mismo nombre que apuntaría a la sofisticación de su programación. La herramienta en cuestión, llevaba en explotación un periodo superior a seis años hasta su descubrimiento y anulación, aunque múltiples derivados serían recurrentemente descubiertos. Kaspersky apuntaría al mismo origen en la programación de los tres virus[592]. Las

---

[589] Sin posibilidad de equívocos, Stuxnet se revelará finalmente como una ciberarma diseñada por la inteligencia norteamericana para sabotear el plan nuclear iraní: http://arstechnica.com/tech-policy/2016/02/massive-us-planned-cyberattack-against-iran-went-well-beyond-stuxnet/

[590] La empresa Symantec elaboraría un informe detallado sobre el funcionalmente de Stuxnet: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[591] Asimismo en el dossier de prensa explica con detalle el mecanismo por el que infecta y daña las instalaciones industriales de las centrifugadoras de gas: http://www.symantec.com/connect/blogs/stuxnet-breakthrough

[592] El análisis forense de Flame, algún tiempo después despejaría buena parte de su supuesta sofisticación, apuntando más bien a las técnicas de introducción que permitieron su permanecía durante años en los equipos infectados: https://windowstips.wordpress.com/2012/06/27/webcast-sobre-flame-o-

revelaciones de Edward Snowden acerca de los programas de espionaje norteamericano pondrían, tiempo después, claridad acerca del origen de estas armas tecnológicas, al confirmar que Stuxnet sería una colaboración entre la NSA e Israel, a través de la FAD (Foreign Affairs Directorate), una sección de la propia NSA que establece trabajos conjuntos con otras agencias aliadas.

La lección más importante en la localización de este nuevo arsenal de ciber-armas, es el reconocimiento de cómo los estados han tomado consciencia del nuevo escenario que supone internet y cómo en este territorio, la guerra no declarada no tiene fin, dado que aún no se han definido los límites ni las formas en las que Internet puede ser escenario bélico. Esta indefinición ha propiciado la extensión de conflictos no declarados a través del entorno digital, aunque la escalada y dimensión a la que se ha llegado en la presente década apunta a que los organismos internacionales de Ciberdefensa, más allá de trazar sus esquemas de seguridad deberán en un momento dado fijar unos principios con los que guiarse, parecidos a las convenciones sobre la guerra auspiciadas por las Naciones unidas.

Sin pretender extendernos en la cronología de esta guerra, el hactivismo también pasaría a la acción, como hemos explicado cuando tratamos de WikiLeaks. Efectivamente, activistas identificados con el colectivo Anonymous desatarían el primer episodio de guerra informática global en 2010 contra empresas de comercio electrónico, como Visa MasterCard o PayPal. La negociación de la ley SOPA (*Stop Online Privacity Act*) en EEUU, desatará el segundo gran movimiento entre 2011 y

---

ponga-amenaza-aqui-para-administradores-it/

2012, frente a esta ley restrictiva sobre los derechos de autor. Estos dos ejemplos nos sirven para ser conscientes que en este conflicto no solo los estados participan sino que ciertas formas de activismo, empresas y delincuentes, confluyen en la estrategia del ataque por medio de la red.

El caudal actual de ataques que diversas empresas de seguridad suministran nos permite hacernos una idea del caudal de recursos movilizados en procesos de relacionados con diversas formas de agresión cibernética. Unas cantidades que nos pueden dar una perspectiva sobre los intereses que este tipo de proceder pueden llevar a motivar. Un incremento en el que como ya hemos apuntado, confluyen diversas fuentes para convertir la red en un entorno en contante conflicto.

Organizando la Ciberdefensa

Cuando en 1993, los analistas estadounidenses John Arquilla y David Ronfedt acuñaran el término *Netwar (ciberguerra), en su ensayo "la ciberguerra está llegando"* todavía no resultaba común reconocer la dimensión que el asunto estaba tomando y su argumentación respecto a cómo las tecnologías del ciberespacio y su evolución cambiarían el modo de concebir y hacer la guerra, no tenía el calado que en nuestro tiempo ha adquirido. Por ello, el texto se nos muestra esclarecedor, ya que apunta claramente la progresiva integración de todos los procesos automatizados de los sectores productivos en la red de redes, facilitando su gestión pero con ello acrecentado las posibilidades de que se exploten las diversas vulnerabilidades inherentes a un sistema totalmente conectado[593].

[593] El documento *La ciberguerra está llegando* es una de las fuentes clásicas de consulta,

Otras de las fuentes fundamentales que suelen ser citadas de manera recurrente al tratar el tema de la ciberseguridad de estados y la ciberguerra en general es él informa elaborado por la OTAN, llamado el Manual de Tallin [594]. Elaborado por el centro de cooperación sobre ciberdefensa (CCDCOE), con sede en Tallin, Estonia, el informe ha sido la fuente principal en casi todos los documentos que hace referencia a la ciberguerra, por ser una de las elaboraciones más detalladas respecto al modo de proceder en un eventual conflicto cibernético. La fuente ha sido duramente criticada por entidades de derecho al proponer, por ejemplo el asesinato de hackers como método de eliminación de oponentes en este tipo de conflictos. Precisamente la falta de acuerdos internacionales al respecto del uso de ciberarmas o el derecho internacional respecto a este tipo de conflictos deja lagunas que permiten este tipo de elaboraciones. Llamadas al orden al respecto como las que Eugene Kaspersky ha realizado, para que se cree algún tipo de regulación respecto a las ciberarmas no han sido respondidas por las autoridades.

En un sentido similar al informe anterior saltarían, a finales de 2012, a la primera línea informativa las declaraciones de Leon Panetta, en aquel momento Secretario de Defensa estadounidense, al alertar sobre la eventualidad de que su país fuese víctima de lo que denominó como *'Pearl Harbor digital',* en clara alusión a las consecuencias que podría tener un ciberataque masivo y coordinado (APT) contra las redes eléctricas, el sistema de transporte o el sistema financiero del país[595]. Este tipo de

---

a pesar de ser de 1993, para establecer los parámetros de la ciberdefensa: www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf

[594] El Manual de Tallin, retirado de la fuente oficial, puede ser consultado en Issuu: http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381

[595] Sobre el *"Pearl Harbour digital*", las declaraciones de Panetta serían uno de los puntos

ataques, estaban ya comenzando a ser descritos como una de las bases de todo proceso bélico, algo parecido al papel que los bombardeos masivos pudieron tener en el siglo pasado. Panetta, no era ajeno al término ni a su uso, si nos hacemos eco a la amplia lista de ataques a los que la lista de "Rouge states" han sido víctimas.

En este escenario de nuevo orden mundial, se desdibuja en parte las potencias que hacen de herramientas de ciberguerra, aunque estados como China, Rusia o Israel, compiten abiertamente con los Estados Unidos en un proceso soterrado de confrontación soterrado. En la actualidad, todos los grandes estados cuentan con agencias, en mayor o menor grado declarado, que se encargan de la ciberseguridad. La frontera entre lo declarado y el espionaje y contratación de agencias externas será la parte principal de los escándalos de espionaje que se denunciarían a lo largo de la segunda década del siglo. A pesar de ello, las estrategias de ciberseguridad son una de las cuestiones en las que los responsables de defensa de las diferentes naciones están volcando sus esfuerzos. En un tiempo en el que la acción militar cada vez tiene mayores limitaciones en sus terrenos de acción, el frente electrónico se ha convertido en la nueva vía de acción no declarada. Como señalábamos, la falta de claridad en los organismos internacionales a la hora de definir y acotar el territorio de la ciberguerra está sirviendo para que ciertos estado saquen provecho de ello para perjudicar a adversarios o imponerse en el plano informático[596].

---

de partida para reenfocar la cuestión en la opinión pública norteamericana, muy dañada en aquel momento por los escándalos de las filtraciones del espionaje cuidadano: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

[596] La última conferencia de la OTAN sobre la ciberdefensa, celebrada en febrero de 2014 en Roma, nos deja una cantidad importante de documentación acerca de cómo ha evolucionado el concepto de seguridad en las redes. La documentación completa está disponible en el enlace: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-

Las agencias de seguridad y espionaje ya vivieron, como hemos visto su particular periodo de reconversión hacia un entorno en el que lo digital se ha convertido en el eje sobre el que pivotan las comunicaciones y la información. Sin embargo, como vimos al tratar el tema sobre el 11S, un abandono temprano de las fuentes de información junto con un perfeccionamiento de las maneras de eludir la vigilancia y conocer los mecanismos de esta hicieron ya en su momento que la inteligencia norteamericana no estuviera suficiente mente preparada para hacer frente a la amenaza yihadista[597].

En EEUU, existe desde 2009 un *cibercomando* operativo dedicado exclusivamente a la Ciberdefensa, dependiente del departamento de Defensa. El general Keith Alexander, es el responsable de este ejército cibernético en reserva para casos de ataques masivos u otras contingencias de tipo cibernético. La eventualidad de un despliegue a gran escala en lo relativo a la ciberguerra ya no es un escenario marginal. EEUU ha sido una de las naciones que más esfuerzo en este sentido han invertido, en parte gracias a la desquiciante política de contratas que lleva adelante y a la profusión de organismos redundantes. De cualquier modo, la división a cargo de este general y la "sopa de agencias bajo sus órdenes" han significado una reorientación en lo que a una organización ofensiva en la red. El USCIBERCOM, y el JFCC-NW (Joint Functional Component Command for Network Warfare), serán los brazos ejecutores mientras que los organismos dependientes de la NSA y la CIA, serán los encargados de

cert/1895-exito-en-la-ix-conferencia-de-la-otan-sobre-ciber-defensa-celebrada-en-barcelona.html

[597] Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

procesar la información que obtengan mediante sus programas específicos, que hemos conocido agracias a las sucesivas filtraciones[598].

La propia armada estadounidense, es un esfuerzo por unificar los métodos de respuesta, liberaría en su momento DsHell, el software Open Source de ciberseguridad que emplea internamente. En este aspecto, avanzaría lo que otros organismos públicos de otras naciones harían, sobre todo tras la experiencia estonia. Este aspecto destaca la importancia que la seguridad en todos los aspectos tiene en la red y la dificultad de delimitar entre ataques e intereses[599].

China tampoco es un país que se haya quedado al margen del despliegue tecnológico y la eventualidad de un conflicto a mayor escala que el que se mantiene en la actualidad a nivel soterrado. A pesar del secretismo que envuelve todos los elementos relativos a su división cibernética, gracias a ciertas informaciones e infiriendo desde ciertos ataques dirigidos, se ha podido ir conociendo su estructura y forma de operar. La empresa Mandiant, especializada en seguridad en la red, sería la primera en apuntar a la infraestructura dedicada a la ciberguerra por parte del ejército Chino.

La denominada *Unidad 61398*, es un conglomerado de especialistas en todas las técnicas de hacking que estarían operando desde 2006 .La mayor parte de sus actividades están enfocadas al espionaje a largo plazo de empresas y entidades extranjeras. Sin embargo, en pleno proceso del escándalo desatado en EEUU a propósito del eventual espionaje de dispositivos de red Chinos, especialmente de la empresa Huawei y ZTE, la

---

[598] Greenwald, G. *Snowden. Sin un lugar donde esconderse*. Ediciones B. Barcelona. 2014

[599] . DsHell: el software open source de ciberseguridad de la armada estadounidense: https://github.com/USArmyResearchLab/Dshell

respuesta organizada contra intereses estadounidenses y la revelación de que ciertas empresas habían sido largamente auditadas de forma oculta, harán apuntar todas las sospechas hacia el cibercomando chino. El informe realizado por la empresa Mandiant apunta a más de 3000 marcadores únicos que confirman ataques organizados provenientes de un lugar concreto de China[600].

Si el caso chino es opaco, la situación de Corea del Norte es todavía más particular. Mucho se ha especulado acerca de fallos en sistemas públicos en Corea de Sur, pero el caso en el que se ha señalado claramente al régimen del ahora presidente Kim Young Hun, será el del masivo ataque a la multinacional Sony. La empresa ya ha sido objetivo de varios ataques importantes a lo largo de su trayectoria de orígenes muy diversos, como ya hemos apuntado en anteriores capítulos, pero el caso más reciente, de 2014, coincidente con la polémica del film *The interview*, que categorizaba de forma cómica al plenipotenciario de Corea del Norte, apuntaría de forma inequívoca a una intervención organizada y planificada. La revelación de buena parte de filmes pendientes o en proceso de realización y el filtrado de documentación confidencial de Sony significaría un capítulo de guerra contra una empresa que no se había manifestado en esta dimensión aún. La definitiva acusación por parte del FBI de ser originario de Corea del Norte y la recopilación de pruebas al respecto, en este caso hechas publicas por el interés estadounidense, serán otra fuente para

---

600 . Resumen de los datos más relevantes sobre la Unidad de espionaje china, recogida por la empresa Mandiant: https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/

El informe detallado sobre este pude consultarse en: *APT1: Exposing One of China's Cyber Espionage* Units: intelreport.mandiant.com/Mandiant_APT1_Report.pdf

determinar el grado de sofisticación que se ha conseguido por parte del hacking dirigido por naciones[601].

Rusia es otra de las naciones que aparte de la establecida cultura hacker dentro de sus nacionales ha sabido organizar una división encargada a la ciberguerra. Como viene siendo habitual, su conocimiento nos llega de forma indirecta en la mayor aparte de las ocasiones. Una de las oportunidades en las que se pudo visualizar con mayor claridad la existencia de esa división dedicada a internet del ejército ruso será la desatada a partir de la llamada Operación Octubre Rojo, en 2013. Con ese nombre la compañía de seguridad informática Kaspersky, denominará a una operación a gran escala de espionaje que llevaría operativa desde 2007. El modelo de explotación mediante infección, llegó a ser tan sofisticado que pudo ser capaz de vulnerar el sistema de cifrado denominado ACID, que emplean organismos como la OTAN y estados de la UE y contar con módulos, al estilo de Flame, para borrase, destruir pruebas y eludir controles. Todas estas características apunarían al FSB, (Servicio Federal de Seguridad) y volverían a identificar las formas en las que la guerra en la red se desarrolla en un sistema sutil de equilibrios y ausencia de declaraciones al respecto[602].

---

[601] Varias fuentes reconocidas recogerían afirmaciones por parte del FBI sobre la intención de los ataques respecto a la retirada del film.

CNN:http://cnnespanol.cnn.com/2014/12/18/corea-del-norte-detras-del-ataque-cibernetico-a-sony-pi

The New York Times: http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?smid=tw-bna&_r=1

Reuters: http://www.reuters.com/article/2014/12/18/us-sony-cybersecurity-attribution-idUSKBN0JV2VL20141218?feedType=RSS&feedName=technologyNews

[602] El informe de Secur List, acerca de la operación Octubre Rojo, detalla el procedimiento de espionaje y las vías de infección de manera bastante pormenorizada: https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/

A nivel Mundial, ya hemos tratado de la Unión Internacional de telecomunicaciones (ITU en sus siglas internacionales) trata de organizar la extensión de protocolos uniformes y en los aspectos de ciberseguridad también cuenta con una oficina dedicada principalmente a le extensión de estándares comunes. Al margen de los polémicos debates acerca de la soberanía de las telecomunicaciones y la propia independencia de la organización, en lo que respecta a métodos de implantación de estándares relativamente seguiros sus tareas de extensión, especialmente entre economías emergentes y en zonas donde la red no se ha desplegado aún, están jugando un papel importante. Aprovechar la extensión de las redes para fijar métodos actualizados, reconocibles y seguros es una de sus principales tareas en este sentido[603].

En Europa ENISA (Agencia Europea de Seguridad de las redes y de la información) es el referente en los aspectos a diseños comunes de estrategias de ciberseguridad del conjunto de sus socios. En general se determinan guías y procedimientos para que sean implantados en los diversos países de la unión y mantiene su propio CERT (Computer Emergency Response Team- Centro de respuesta a emergencias) en contacto con los CERT de los estados miembros[604].

---

[603] . La UIT (ITU en sus siglas internacionales) mantiene una actividad intensa en los aspectos de extensión de las telecomunicaciones en el ámbito global: https://www.itu.int/es/Pages/default.aspx

[604] La documentación general sobre buenas prácticas y el esquema de recomendaciones que ENISA da a los estados que la componen, es una fuente sobre la orientación hacia la seguridad que el organismo europeo pretende : http://www.enisa.europa.eu/activities/risk-management/evolving-threat-

EN el aspecto militar, Europa por si misma está trabajando en una estrategia común de Ciberdefensa. La Agencia Europea de Defensa es el organismo de corte militar que trata de compatibilizar la pertenencia de la mayor parte de los estados miembros en la OTAN con una estrategia europea capaz de definición propia. En los aspectos de ciberdefensa, se ha diseñado desde 2013 una estrategia común para los estados miembros. El peso de las revelaciones sobre espionaje entre estados aliados, ha motivado el impulso de este tipo de medidas entre ciertos estados miembros que ven en la estrategia común una forma de establecer un desarrollo independiente del patrocinio estadounidense[605]. Como la mayor parte de este tipo de documentación, aparte de las declaraciones de intenciones y las presentaciones públicas, las fuentes de los auténticos diseños nos suelen llegar mediante diversos tipos de filtraciones. Así ha sido el caso del diseño de esta estrategia para los periodos del quinquenio 2015-20, que la ONG *Statewach* ha conseguido obtener, analizar y publicar[606].

La ciberseguridad en España, de un punto de partida prácticamente inexistente o enfocada eminentemente a los aspectos de defensa e interior más que en la elaboración de estrategias de ciberdefensa propiamente dichas, ha pasado a elaborar un abanico de sistemas y organización similares al de países de nuestro entorno[607]. El Instituto nacional de

---

environment/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure/iitl

[605] Estrategia Europea de ciberdefensa (diseñada a lo largo de 2013 y puesta en marcha en 2014: http://www.eda.europa.eu/info-hub/news/2015/07/13/military-requirements-for-cyber-ranges-agreed

[606] La renovación de la política común de ciberdefensa por el periodo 2015-2020 ha sido filtrado y publicado por Statewach*: http://www.statewatch.org/news/2015/aug/eu-docs-iss.html*

[607] La preocupación por la elaboración de protocolos y planes de contingencia respecto a la ciberseguridad en España es algo relativamente reciente: http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL

Ciberseguridad, INCIBE, antes INTECO, es el organismo estatal encargado de las cuestiones de ciberseguridad y las garantías generales en el entorno de la red[608]. Entre los servicios que presta, la alerta temprana sobre virus y contingencias y servicios a ciudadanos y pymes y los planes de prevención y extensión de una cultura de la seguridad informática son de sus aspectos destacados. Entre sus secciones más importantes, la Oficina de Seguridad Informática (OSI) En los aspectos dedicados al ciudadano[609]. En lo relativo a la industria el CERTSI (CERT de Seguridad e industria) se dedica a los ámbitos productivos y la empresa, como centro de respuesta[610]. Por último ENISE es el encentro anual donde profesionales y especialistas del ámbito de la seguridad revisan las estrategias anuales en lo que respecta a la ciberseguridad. En octubre de 2015 celebra su novena edición (39).

En el terreno Interno, el Centro Criptológico Nacional (CCN-CERT), dependiente del Ministerios del Interior, es la entidad encargada tanto de establecer los parámetros de la estrategia nacional de Ciberseguridad, algo que hasta 2012 no existiría en nuestro país y que la emergencia de cada vez más sucesos relativos a la seguridad impondría en una agenda acelerada, y el velar por las infraestructuras esenciales del estado[611]. Como declaran, su principal objetivo es contribuir a la mejora del nivel de seguridad de los sistemas de información de las públicas, para ellos aspiren a convertirse en el centro de alerta nacional cara a los sistemas de la administración y ser el CERT de referencia en este aspecto.

_CONTEXT=/elcano/elcano_es/zonas_es/defensa%20y%20seguridad/ari102-2010

608 El INCIBE, como organismo de referencia en la seguridad de la información es un organismo dependiente del ministerio de industria: https://www.incibe.es/

609 OSI: http://www.osi.es/

610 CERTSI: https://www.incibe.es/blogs/incibe/Seguridad/BlogSeguridad/ultimos_articulos/

611 ENISE: https://www.incibe.es/enise/

La documentación pública que genera esta entidad es de las más claras y valoradas actualmente y posee su propia certificación que busca uniformar la gestión de incidencias y la actualización de conocimientos[612]. La elaboración del esquema nacional de seguridad es una de las fuentes de referencia a la hora de establecer unos parámetros reconocibles por todo el sector público y una guía para el privado[613].

Como vemos, a lo largo de todo el mundo las naciones han tomado consciencia de la importancia de elaborar estrategias de ciberdefensa de forma acelerada. Las fuentes de todas estas elaboraciones parten en buena medida de las experiencias de conflictos recientes y las reacciones de profesionales del entorno. Así el proceso de adquisición de conocimientos y el incremento y militarización de los efectivos dedicados exclusivamente a conocimientos de hacking[614]. Sin pretender extendernos en las diversas elaboraciones de un movimiento muy reciente y de plena actualidad, organizaciones como THIBER en España, han elaborado unas buenas síntesis sobre el estado de la cuestión[615].

---

612 CNN- CERT (Centro Criptológico nacional- Gobierno de España) Informe de ciberamenazas 2014 y tendencias 2015. Recurso disponible en: https://www.ccn.cni.es/index.php?option=com_content&view=article&id=18&Itemid=22

613 CNN- CERT (Centro Criptológico nacional- Gobierno de España): Guías del esquema Nacional de Seguridad: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

614 . El Real Instituto Elcano, en colaboración con THIBER *(The Ciber Security Think Thank*) mantiene una serie de informes mensuales sobre ciberseguridad en los que colaboran los más destacadas personalidades del sector. Los informes están disponibles en: http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/publicaciones/ciber-elcano/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP0os3jjEBf3QG93QwMLQwNLA0dfD7PAwABXI-8QI_2CbEdFAMWyODY!/

615 THIBER (The Ciber security Think thank) es una organización que se encarga de difundir la importancia de estrategias de ciberseguridad entre gobiernos y empresas. Mantienen en su sitio una recopilación de artículos e informes al respecto muy interesante

La escalada en ciberseguridad

Como asegura Jesús Martín Barbero, vivimos en un periodo de fundamentalización del concepto de seguridad. Efectivamente la tensión entre lo sucedido en 11 S y lo que, por ejemplo, representa el Foro Social Mundial no debería ser de ninguna forma ligado. Sin embargo, a lo largo de esta tesis hemos podido ver la multitud de ocasiones en las que supuestos organismos dedicados a la seguridad, bajo el alegato del terrorismo, han enfocado sus recursos y esfuerzos a la vigilancia ciudadana o el espionaje[616]. El aumento de recursos dirigidos a la seguridad ha vivido varias oleadas que van desde el interés primero de gobiernos y grades empresas hasta ir bajando de nivel hacia empresas menores y usuarios particulares. El propio avance de las amenazas y el aumento de la criminalidad en la red, han propiciado que profesionales dedicados a la seguridad informática tengan que mantener una tensión permanente en el conocimiento de las herramientas de hacking y el diseño de planes de contención y seguridad[617].

Todo este proceso ha significado para la mayor parte de las naciones una adaptación acelerada a una realidad que se ha impuesto por la vía de los hechos. La cantidad de incidentes en empresas y estados se han multiplicado hasta extremos en los que las naciones han tenido que establecer sus diseños con carácter de urgencia. Por un lado, el terreno de la seguridad había sido desatendido. La mayor parte de la inversión que se destinaba a procedimientos activos de intervención más que al consolidado de infraestructuras y diseño de principios de reacción antes

---

disponible en: http://www.thiber.org/articulos/

616 VV.AA. *Sociedad Mediatizada*. Gedisa. Barcelona.2007

617 Greenwald, G. *Snowden. Sin un lugar donde esconderse*. Ediciones B. Barcelona. 2014

contingencias[618]. La dependencia tecnológica, producto de un servilismo hacia la gran empresa, mayoritariamente norteamericana, la crisis económica y el estado de maduración del conocimiento de la red actual por parte de entornos dedicados a la seguridad y el hacking en general, han llevado en los últimos años a una situación de "tormenta perfecta " en cuanto a incidentes de seguridad. Todos los días son publicadas diferentes vulnerabilidades de sistemas informáticos para los que no se actualizan ni siquiera infraestructuras críticas. Esto significa que no solo ya grandes conjuntos de hackers con conocimientos avanzados y dedicación puedan explotarlas sino que simples aficionados con cierto nivel, pueden llegar a explotarlas y tener acceso a recursos privados de empresas y organismos críticos[619].

La proliferación de mecanismos capaces de tener acceso pleno a sistemas e información crítica, desde que la movilidad se ha extendido entre toda la población y la extensión de modelos BYOD (Bring Your Own Device- tráete tu propio dispositivo) en cierta cultura de empresa, ha aumentado exponencialmente la exposición al hackeo de sistemas críticos. Este crecimiento de eventos críticos, ha puesto en una situación de exposición a la empresa y organismos que no cuentan con planes de contingencia ni con profesionales y mecanismos para una respuesta adecuada. La extensión de medios criminales de acceso a recursos ajenos, debe mucho a la extensión de una cultura de la desatención que no solo está entre usuarios sino que la propia empresa no es consciente hasta que no es atacada. Los casos de *Ransonware*, del secuestro de información, de los ataques tipo APT, ataques dirigidos de forma

---

[618] Gobierno de España (2013). Estrategia de Seguridad Nacional: un proyecto compartido (10/05/2013) : http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

[619] . Peña, R. *Cuadernos de consultor para el curso de experto universitario en hacking ético de sistemas*. UDIMA. Madrid. 2015

persistente, con el objeto de introducirse en una red empresarial u obtener datos concretos, son una fuente cotidiana de las empresas de ciberseguridad, que ven como la mayor parte de organismos y empresas no tiene trazado ningún mecanismo de reacción para tales contingencias[620].

La normativa UNE/ISO-27001 y todas las derivadas, hacen mención expresa a las formas en la que la seguridad de la información debe organizarse en entornos de redes informáticas. Sin embargo, es extraño aún que empresas de cierto nivel tengan responsables de seguridad o medios dispuestos a establecer estos mecanismos, especialmente tras la cultura de la "subcontrata" establecida al calor de la crisis económica iniciada en 2008. La importancia de elaborar estándares en los que a sistemas de gestión de la seguridad de la información, está viviendo en los últimos años un periodo de concreción que el general de los profesionales del tema veía necesario[621]. La adecuación de las normas del derecho es otra de las cuestiones en las que se vive un proceso acelerado en lo que respecta a la elaboración de normas[622]. En el terreno en el que estamos tratando, la celeridad es un elemento fundamental y la fluidez en la captación de pruebas, la obtención de permisos judiciales y la colaboración de empresa y agentes implicados son fundamental.

---

[620] Clapper, James R. (2013*).Worldwide Threat Assessment of the US Intelligence Community.* En: Office of the Director of National Intelligence, de 12 de marzo. Disponible en: http://intelligence.senate.gov/130312/clapper.pdf (27/05/2013).

[621] La norma UNE/ISO-27001 es la que hace referencia a los Sistemas de gestión de la seguridad de la información. Su certificación pasa por ser un requisito cada vez más necesario para la empresa: http://www.aenor.es/aenor/certificacion/seguridad/seguridad_27001.asp

[622] . De la anterior norma, derivan una serie de recomendaciones y normas de desarrollo hoy en día en pleno proceso de elaboración y consolidación y que supondrán las bases para establecer parámetros seguiros en las redes: http://www.aec.es/web/guest/centro-conocimiento/norma-une-isoiec-27001

Mientras las agencias de inteligencia estatales han procedido a expandir las formas de adquirir conocimientos mediante una red cada vez más intervenida, en el apartado de la respuesta a estos mismos procesos provenientes del exterior todavía no se había elaborado con la misma intensidad. La capacidad defensiva no avanzaría al mismo ritmo que el interés por la captación y penetración de sistemas ajenos. En este sentido, las formas de operar de las agencias estatales dedicadas a la inteligencia han podido ser asimiladas al proceder del cibercrimen, y bajo esa premisa son tratadas por buena parte de los profesionales y empresas dedicadas a la seguridad[623]. Efectivamente, independientemente de la procedencia, una amenaza tipo APT, ataque persistente para exponer datos de la víctima, un ataque DDoS, o una infección de malware, por poner ejemplos

---

[623] Actualmente contamos con seis grandes mapas interactivos de análisis de ciberataques en tiempo real. Su consulta nos puede hacer una idea del grado de concurrencia y sofisticación de las ciberamenazas. Asimismo, nos ofrece una fuente histórica para poder ubicar momentos concretos que queramos destacar o conocer:

- Cbertrath de Kaspersky. que aporta un análisis en tiempo real de cómo se producen los ataques que detectan mediante su herramienta: https://cybermap.kaspersky.com/
- Digital attack map: que nos muestra un mapa de los ataques DDoS: http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=16659&view=map
- Norse. También perteneciente a una empresa de seguridad y que detalla muy correctamente el origen, frecuencia y envergadura de los ataques : http://map.ipviking.com/
- Honey Net. Un mapa interactivo, http://map.honeynet.org/
- *Sicherhe its tacho*. de una empresa alemana dedicada a la seguridad de empresas: http://www.sicherheitstacho.eu/?lang=en
- Gráficas sobre ataques y cargas de Internet a nivel mundial http://www.akamai.com/html/technology/dataviz1.html

reconocibles, son sin importar la procedencia amenazas a las infraestructuras frente a las que hay que intervenir activamente y bloquearlas[624].

La guerra contra el terrorismo

Después de la amenaza de naciones, la delincuencia y el activismo hacker, el terrorismo es la última cuestión que cerraría el cuadro de la ciberguerra. La fuente del terrorismo cerraría el itinerario de amenazas que conforma este escenario global de ciberguerra. Sin embargo, a pesar de su importancia en otros planos, veremos como en la red, apenas pasan de ser asimilables a lo largo del perdió como episodios puntuales de hacking de servicios y daños muy localizados y puntuales. Así, más allá de la imagen que pudiéramos imaginarlos, la acción del terrorismo en la red, apenas se aproxima a la que colectivos de hackers hayan podido producir en los primeros años de la segunda década de nuestro siglo. El carácter de sus componentes y la forma de emplear la red para acciones de corte terrorista fuera de la red son los que conforma realmente esta amenaza que cada vez es más ampliamente analizada. Por tanto en la lucha contra el ciberterrorismo la fuente es más bien transversal, al emplearse la red no cómo método exclusivo sino como medio de comunicación social entre sus elementos[625].

---

624 . Otra fuente más analítica de los ataques su origen e intención nos la ofrece la web Hacmageddon: http://www.hackmageddon.com/category/security/cyber-attacks-statistics/

625 . Diana Barrantes, de Instituto Elcano, nos hace una excelente introducción sobre las fuentes y formas de organización del terrorismo y de su empleo de medios tecnológicos en: ¿Cuál es el alcance del ciberterrorismo? http://www.blog.rielcano.org/cual-es-el-alcance-del-ciberterrorismo/

Mientras en la mayor parte de occidente, la desaparición de grupos terroristas de índole nacional ha sido una pauta común, hasta llegar prácticamente a la inexistencia, desde el 11S la trascendencia del terrorismo de corte extremista islámico ha adquirido una dimensión internacional .La amenaza permanente de esta nueva dimensión del terrorismo de corte yihadista ha sido la piedra de toque de las organizaciones de defensa nacional. Precisamente es el tiempo en el que estos grupos se han creado lo que condiciona sus métodos y por tanto no nos debe extrañar que el empleo de la red para la consecución de sus fines sea común[626]. Hasta tiempos recientes, Internet ha sido empleado por grupos terroristas con mucha precaución. La utilización de herramientas de cifrado de contenidos y comunicaciones y el uso prudente de medios tecnológicos ha permitido que las organizaciones no comentan muchos errores en cuanto al revelado de sus estrategias por medios informáticos. Los casos en los que se han cometido errores, sobre todo los que Israel publica, son ocasiones muy reconocibles por las consecuencias para quien hace uso de alguna tecnología que permita ubicarle.

Las tareas de proselitismo y propaganda de diversos grupos de terrorismo islamista ha sido una de las herramientas más utilizadas. La recurrente creación de cuentas de apoyo a estos grupos `para dar a conocer sus acciones en diversas redes sociales y la difusión de vídeos con sus atentados no solo sirve a esta tarea a través de los medios

[626] La Oficina de las naciones unidas sobre drogas y crimen (UNODC), con sede en Viena, publicarían un extenso informe sobre el Uso de internet para fines terroristas que puede ser consultado en su web: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

informativos clásicos sino que emplea la red como plataforma[627]. La dificultad para cerrar cuentas que de forma recurrente vuelven a ser creadas, ha disparado las alertas en ciertas redes sociales como twitter o Facebook y en otros enfocados al video como YouTube, que tratan de retirar los contenidos con la mayor premura. En el sentido del uso de redes sociales y elementos de la red para provecho de sus infraestructuras es donde los medios de seguridad de los estados más pueden intervenir. En el caso español, el Plan Estratégico Nacional de Lucha contra la Radicalización Violenta, es una fuente reconocible de esta estrategia[628].

En lo que respecta a la acción terrorista propiamente dicha por medios de la red, grupos de apoyo al estado islámico han sido los primeros en plantear estrategias similares al as que a lo largo de 2012, hicieran grupos como Anonymous o Lulzcsec. Así la explotación de vulnerabilidades en medios en la red, sobre todo en páginas web no convenientemente securizadas o sin actualizar conveniente, han propiciado la suplantación de servicios o el hackeo de cuentas que se han empleado principalmente como medio de propaganda. Milicias palestinas como Hezbollah, comenzarían a organizar sus comandos de agentes especializados en hacking, para establecer campañas de corte propagandístico. Incluso se ha llegado a afirmar que estos cuentan con hackers rusos, contratados en el mercado negro para la consecución de sus acciones. Por su parte, grupos

---

[627] Sobre el empleo de redes sociales por parte del extremismo islámico, se ha debatido mucho en medios y conferencias al respecto, al ser una de las cuestiones en las que estos tienen más capacidad de eludir controles y actuar. http://foreignpolicy.com/2013/02/05/jihads-social-media-trend/

[628] Plan Estratégico Nacional de Lucha contra la Radicalización Violenta:

http://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/300115-enlaceradical.aspx

autodenominados Anonymous, también acudirán contra la barbarie de ciertos actos de estos grupos y dirigirían sus ataques contra el estado Islámico y los grupos de apoyo al terrorismo. La campaña denominada #OpIceISIS, de cuyo alcance y consecuencias no se pudo saber mucho más, es un ejemplo de cómo se han terminado por entrecruzar diversos grupos que actúan en la red con fines radicalmente distintos[629].

Por su lado la *Syrian Electronic Army*[630], ha sido una de las organizaciones decididamente terroristas que más acciones del tipo hacking han llevado a cabo. En 2013, un ataque coordinado a medios de información como la BBC, France 24 TV, diversas radios públicas estadounidenses, Al-Jazeera, el Gobierno de Qatar y diversas cuentas de Twitter consiguió mediante la difusión de informaciones falsas desde estas cuentas intervenidas que cierto público se hiciera eco estas y llegaría incluso a provocar una caída de 145 puntos al índice Down Jones[631].

Otros grupos como la ciberguerilla Izz ad-Din al-Qassam, también acudirán a métodos del hacking reivindicativo para pasar a operaciones de sabotaje bancario en EEUU. La mayor parte de sus ataques se producen mediante los conocidos sistemas de ataque DDoS, contra infraestructuras por tanto no debidamente actualizadas. Parece ser que en este caso la guerrilla tendría una vinculación estrecha con el estado Iraní y que por tanto

---

629 . La pintoresca declaración de guerra contra el estado islámico por parte de Anonymous permanece en su vídeo de YouTube y aunque sea una forma muy empleada por este grupo de colectivos merece contar con una muestra para conocer cómo la red es un lugar de reto y escaparate de estos grupos:

https://www.youtube.com/watch?v=_kJtvFUMELM

630 La Sirian Electronic army sigue contando en twitter con un medio propio, cuya cuenta sigue activa al día de la redacción del presente trabajo: https://twitter.com/Official_SEA16

631 La cadena *France 24* daría cuenta del impacto del ataque: http://www.france24.com/en/20150409-france-tv5monde-is-group-hacking

respondería más a una estrategia de respuesta difusa a las intervenciones de EEUU que a grupos autónomos o células terroristas.

La auténtica guerra que plantea el terrorismo de corte islámico, especialmente el ISIS[632], se juega en el terreno de la propaganda. Así, se ha podido determinar que a través de una investigación sobre el censo de cuentas en twitter vinculadas a este grupo que podría tener del orden de 46.000[633]. Periodistas como Gary Bunt, llevan años realizando un seguimiento de la actividad del islamismo más extremista y la evolución de sus sectores propicios al terrorismo, fundamentalmente enfocados a la propaganda. El esmero con el que son presentados los vídeos de las "acciones" terroristas, especialmente en lo que respecta a suicidas, con una edición cuidada (casi cinematográfica), apunta a su doble objetivo de amedrentar al enemigo ioccidental y de servir de proselitismo avalando modelos de conducta a seguir por futuros "mártires". Este exhibicionismo, ha fomado parte sustancial del proceder del Daesh desde su defección de Al Qaeda y es una de las partes mas reconocibles de su acción concreta en la red.

A pesar de ello, la difusión del *Manual del Terror,* tendría especial impacto en la red, al tararse de una guía detallada de cómo realizar atentados y de las formas de actuar en la red por parte de miembros de grupos terroristas islámicos [634] . Sobre el tema de la

---

632 Carlini, A. *ISIS: Una nueva amenaza en la era digital.* Informe disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO129-2015_ISIS_AmenazaEraDigital_AgneseCarlini.pdf

633 Estudio sobre la creación de cuentas del ISIS tras su escisión de Al Qaeda: http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf

634 . Virtual Islamic, el blog que realiza un seguimiento del islamismo en la red: http://virtuallyislamic.blogspot.com.es/

propaganda extremista, especialmente focalizada a la actividad del autoproclamado Estado Islámico o ISIS (más correctamente conocido DAESH), se han realizado estudios al rspecto de la repercusión de esta propaganda y su capacidad real de rposelitismo. Así, aunque el efecto y la cuidada imagen que tratan de confrontar respecto a occidente, con la proliferación de memes y la ya citada profusión de cuentas en redes como Twitter, la realidad es que el impacto en lo que respecta a la captación por estos medios de nuevos acólitos resulta ostensiblemente baja [635]. El seguimiento realizado de dichas cuentas por parte del diario británico The Independent[636], especialmente tras los antentados de parís y las sucesivas campañas de denuncia a cargo de activistas y de bloqueos por parte de la empresa de microblogging, han hecho que los miembros realmente interesados en esta porpaganda comiencen a migrar a otras redes, especialente grupos cerrados de Telegram. En este sentido, Twitter trataría de reaccionar tras ser sucesivamente señalada como una de las redes mas activas del terrorismo islámico y elevaría un comunicado en el que rinde cuentas de su campaña de cierre de cuentas y seguimiento de elementos afines al terrorismo[637].

---

[635] El estudio sobre la propaganda del DAESH en Twitter, *Occasional Paper The Islamic State's Diminishing Returns on Twitter : How suspensions are limiting the social networks of English speaking ISIS supporters* publicado por J.M. Berger y Heather Perez , a cargo de la Universidad norteamericana George Washington , se encuetra disponible en: https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf

[636] Seguimiento de las cuentas de Twitter del Daesh y la migración de sus miebros activos hacia otras redes sociales no públicas, a cargo del diario The Independent: http://www.independent.co.uk/life-style/gadgets-and-tech/isis-twitter-daesh-islamic-state-isil-propaganda-video-a6880746.html

[637] El comunicado de Twitter, servirá como respuesta a las sucesivas acusaciones de pasividad de la red de microblogging frente a la propaganda que el Daesh fomentaba a través suya: https://blog.twitter.com/2016/combating-violent-extremism

El servicio de mensajería Telegram, demostraría mayor agilidad, al proceder al cierre de grupos, bots (robots que automatizan tareas en la red) y cuentas vinculadas a estos grupos con un éxito relativo aún[638], dado que usuarios individuales, al igual que números de teléfono, no pueden ser retirados si no son inequívocamente identificados como vinculados a practicas de terrorismo. Una de las claves para entender esa transformación en las comunicaciones es el empleo cada vez mayor de técnicas esteganográficas (ocultación del mensaje original). Mucho se habló del empleo de redes y páginas dedicadas a la pornografía[639] para insertar mensajes y comunicaciones entre sus miembros. Asimismo también se ha apuntado al empleo de chats y foros dedicados a ciertos videojuegos,como Call of Duty o GTA y mas recientemente entre los de rol masivo con tecnología móvil y por último el empleo de redes sobre medicamentos y medicina en general, este último en grupos creado en Telegram.

Hasta hace bien poco, ninguno de los ataques que reivindican diferentes grupos vinculados en mayor o menor medida a grupos terroristas han conseguido que sus acciones tengan consecuencias más allá de las propias de la suplantación y el asalto a páginas webs de medios de comunicación o ataques de denegación de servicio a estamentos y bancos no convenientemente actualizados. Por ello, aunque suele ser una fuente común, tratar sobre la amenaza ciberterrorista, la realidad anterior a 2016, era que el ciberterrorismo apenas había pasado de un enunciado y las auténticas fuentes de consecuencias físicas y palpables han sido las producidas con el patrocinio más o menos expreso de diversos estados. A

---

638 La capacidad de bloquear grupo dependerá de cómo estos se expongan: http://securityaffairs.co/wordpress/42096/cyber-crime/telegram-messaging-service-isis.html

639 Sobre la ocultación de información en archivos pornograficos se pudo saber mas tras la incautación de este tipo de material en la base de Bin Laden, según la publicación Wired: http://www.wired.com/2011/05/we-have-found-bin-ladens-porn/

pesar de ello la potencialidad de un avance en este terreno, ante la facilidad que la extensión de las redes ha conseguido en nuestro tiempo, hace que las estrategias frente a tales eventualidades crezcan y que los medios de prevención y respuesta contemplen la posibilidad de un crecimiento en la escala de estos ataques[640].

Otra de las cuestiones planteadas recurrentemente es la enventualidad del empleo de redes ocultas por parte de grupos terroristas. Parece ser que tales efectos tienen poco impacto entre los miebros de tales grupos, dado que tanto el grado de conocimiento como el resultado real obtenible, les disuade de su empleo de forma exclusiva.[641]

La amenaza potencial de este tipo de acciones terroristas ha venido a confirmar lo que se avanzaba como futuros posibles de este tipo de amenazas. Efectivamente, a inicios de 2016 los ataques a Ucrania[642] e israel[643], focalizados en centrales de distribución eléctrica y el posterior ataque a una planta potabilizadora de aguas en Reino Unido[644], nos

---

[640] Como añadido, el artículo, Cinco escenarios de ciberguerra en el nuevo orden mundial tendría una gran difusión en la red gracias a su licencia Creative Commons y al tema tratado. En este detallo las principales fuentes de conflicto cibernético de la actualidad y su posible devenir: Andrades, F. (2013).Cinco escenarios de ciberguerra en el nuevo orden mundial. Disponible en: http://www.eldiario.es/turing/escenarios-ciberguerra-nuevo-orden-mundial_0_129837338.html (8/05/2013).

[641] Documento sobre los usos más comunes de la denominada Dark Web y el escaso impacto en esta de contenidos y comunicaciones de corte islamista: http://securityaffairs.co/wordpress/45755/intelligence/dark-web.html

[642] Detalles por parte de Ontinet, de lo que se conoce sobre el ataque a Ucrania: http://blogs.protegerse.com/laboratorio/2016/01/21/nueva-oleada-de-ataques-contra-la-industria-electrica-de-ucrania/

[643] Sobre el ataque a Israel es sobre el que existen hoy en día mayores sospechas a propósito de una posible autoría: http://globbsecurity.com/ciberataque-red-electrica-israeli-37626/ mas información en: http://thehackernews.com/2016/01/power-grid-cyberattack.html

[644] Sobre el ataque, podemos consultar el informe de verizon http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf En Castellano, el Blog de seguridad Suegur-Info, también recopliaría información al respecto:

llevaran a un escenario en el que este tipo de ataques a través de las redes comienzan a concretarse en amenazas mas que potenciales.

http://blog.segu-info.com.ar/2016/03/hackean-una-planta-potabilizadora-y.html

4.4 Redes sociales, clicktivismo y primaveras de mensajería instantánea.

Cada vez con mayor intensidad, la red es el escenario preferido para el negocio y el conflicto. La acelerada integración social y económica hacia una interconexión y un acceso inmediato, condiciona y marca las formas en las que la nueva sociedad se define. El proceso ha sido tan acelerado que la misma sociedad apenas ha sido consciente, devorada por la inmediatez y el ritmo de asunción de la novedad. El contexto en el que se vertebra la hegemonía en lo que respecta al acceso a la información ha comenzado un proceso de cambio en el que la propia sociedad tiene la opción de jugar un papel activo. La aparición de redes horizontales, en las que el medio de información tan solo es un referencia y quien lo difunde tiene un papel tan activo como el propio informante, junto con la propia manera de comunicarse, de forma masiva e instantánea ha supuesto un vuelco en la forma en la que nuestra sociedad pone en común la información y la distribuye[645].

Las lecciones de momentos puntuales, como el reconocido "pásalo" que vertebraría una respuesta colectiva de la población, días antes de las elecciones y tras el atentado en la estación de Atocha en Madrid el 11 de marzo de 2004 frente a una información manipulada que no se sostenía, han dejado una profunda huella sobre la capacidad de organizarse de la sociedad de nuestros días. Todo ello con las bases de una comunicación todavía en las puertas de Internet, cuyo proceso de

[645] . Ugarte de, D. *El poder de las redes*. Colección Biblioteca de las Indias. Madrid. 2011

extensión se basaría en la capacidad de mensajería SMS de los dispositivos móviles del momento[646]. Según datos suministrados por el operador Telefónica, el tráfico de SMS del sábado se incrementaría en torno a un 20% del habitual en ese momento y el mismo internet también tendría incrementos significativos. El envío masivo de estos mensajes, contradiciendo el argumentario oficial, con unos medios en general bastante volcados en su difusión, fomentará el efecto multiplicador de estos. Un sistema que sería suficiente para convocar todo un conjunto de concentraciones en respuesta a un gobierno que quedaría deslegitimado y terminaría por provocar una movilización capaz de dar un vuelco electoral que ninguna estimación hubiera previsto[647]. Con la perspectiva de los datos disponibles, se puede reconstruir una secuencia que corroboraría la reacción ciudadana y la justificada movilización, dado que los tiempos de incertidumbre fueron realmente ajustados y la tesis de una autoría de ETA insostenible[648].

La primera lección de esta nueva capacidad de organización social alternativa a los medios convencionales apuntará en España a la crisis de los medios de comunicación masivos existentes, como ya hemos señalado en capítulos anteriores, en los que los gobiernos se han apoyado como plataforma propagandística hasta el extremo de quebrar su credibilidad. Por otro lado, la misma sociedad, ha comenzado a informarse y difundir informaciones a través de medios más directos, rápidos y eficaces, con las redes sociales como su punto fundamental. En España, este será el primer capítulo de una organización social desde la base cuya

---

646 VVAA. *Pásalo. Relatos y análisis sobre el 11M y los días que siguieron.* Traficantes de sueños. Madrid. 2014

647 . El informe de David de Ugarte, titulado, "*11M: Redes para ganar una guerra*", también analiza el impacto de las comunicaciones alternativas a los medios tradicionales: https://lasindias.com/gomi/informes/11m.pdf

648 Castells, M. *Comunicación y poder.* Alianza Editorial. Madrid. 2009

trayectoria todavía está por definirse pero que ya, con los movimientos como el 15M y las primeras candidaturas ciudadanas suponen una forma completamente distinta de interrelación social. El movimiento 15M será la siguiente oportunidad en la que las nuevas formas de comunicación social se evidenciarían en la serie de concentraciones y manifestaciones que serían las acciones más evidentes del movimiento. La capacidad de establecer nuevas formas de comunicación entre colectivos mucho más avanzados en el empleo de nuevas tecnologías resultaría fundamental en la forma de organizarse en todas las acciones que caracterizaran al movimiento[649].

Pero en este resurgir de la ciudadanía también hay cuestiones que ensombrecen los movimientos como son la pertenencia de las herramientas de comunicación a empresas radicadas en Estados Unidos. El peaje publicitario y el propio entorno cada vez más dirigido de estos portales junto con el proceso acomodaticio de quienes sustituyen la militancia por el comentario social son la contraparte de este proceso. El denominado *clictivismo*, el activismo a golpe de ratón, es una de las críticas más sustanciales a todo este proceso de expansión de las comunicaciones sociales en el ámbito de la toma de conciencia y la acción política[650].

Nuevas formas de activismo a través de la red y censura

En el terreno contrario, guerrillas tan incruentas como la del Ejército Zapatista de liberación Nacional (EZLN), activa desde 1994, en el estado mexicano de Chiapas, han sabido, de la mano del

[649] Sánchez de Almeida, C. República Internet. Un libro en formato Blog (con entradas hasta julio de 2013) http://republicainternet.com/

[650] Assange, J. *Cypherpunks. La libertad y el futuro de internet*. Deusto. Madrid. 2014.

Subcomandante Marcos, emplear la red como forma de darse a conocer y mantener una tensión mediática desconocida hasta el momento, llegando a crear una red de simpatías que llevaría al gobierno de dicho país a paralizar las operaciones militares contra esta. La clave de su discurso, se basa en un debate que parte de la situación local de subdesarrollo, para llegar a la conclusión de que es la misma globalización neoliberal la que condena a zonas como esta y por tanto, es la respuesta global, la única forma posible de articular una alternativa. De hecho, buena parte de la amalgama de movimientos que conformarían el *Foro Social Mundial* (FSM) en su primera convocatoria en la ciudad brasileña de Porto alegre, partirían de los llamamientos en este sentido propuestos por el propio subcomandante Marcos. La denominada Netwar, o guerrilla informacional, como forma de respuesta social organizada en torno a las redes globales comenzará, de este modo, a surgir en los años noventa del siglo pasado, en el que podemos destacar varios hitos esenciales para conocer su evolución[651]. El primero de estos sería la convocatoria por parte del EZLN en 1996 de lo que denominaría *encuentro intergaláctico,* en el que se trazarán las líneas maestras de estas nuevas formas de organización y confluencia de movimientos en alianzas heterogéneas. El mismo año se celebrará el Social Watch y en junio de 1999, a partir de un artículo de Ignacio Ramonet[652] en su revista *Le Monde Diplomatique,* surgiría ATTAC (movimiento internacional para el control democrático de los mercados financieros y de sus instituciones)[653]. El 30 de noviembre de ese mismo año, acontecería uno de los hitos más reconocidos en la gestación de la primera confluencia mundial de organizaciones alternativas a la

---

[651] VVAA. *Internet y Lucha política: Los movimientos sociales en la red*. Capital Intelectual, Buenos Aires, 2006

[652] Ramonet, I. *Pensamiento único y nuevos amos del mundo*. Icaria. Barcelona. 2008

[653] La organización ATTAC, destacaría por sus elaboraciones en el terreno económico: http://www.attac.org/

globalización de corte neoliberal, como será la denominada B*atalla de Seattle*, donde se concentrarían multitud de grupos antiglobalización de todo el mundo bajo el denominador común de una protesta frente a las pretensiones de la Organización Mundial del Comercio (OCM) y que derivaría por un lado en una auténtica protesta global y a gran escala, como no se conocía en décadas y en los primeros indicios de gestación de un contrapoder mundial apoyado en los nuevos recursos tecnológicos para organizarse de forma horizontal, con nuevas herramientas propias del contexto cambiante característico del momento actual. Uno de los ejes de esta nueva forma de organización será *Indymedia*[654], como agencia libre de noticias alternativas a los medios de difusión privadas. En 2001, el Primer Foro Social Mundial, celebrado en la ciudad Brasileña de Porto Alegre, que se había convertido ya en un referente mundial al establecer por vez primera la elaboración de unos presupuestos participativos, en los que colaboraban anualmente alrededor de un millón de habitantes de la cuidad[655]. A partir de ese primer foro, las convocatorias se harán casi en paralelo a las del foro de *Davos*, como forma de establecer una alternativa global a las propuestas prácticamente unívocas de los organismos económicos internacionales y en la práctica ha supuesto una de las bases del surgimiento de gobiernos de una izquierda diversa en Latinoamérica, tras largas décadas de dictaduras e intervencionismo[656]. Redes similares surgirían pronto en España, como es el servidor *Nodo 50* [657], convertido en

---

654 Inymedia sería una de las primeras páginas en recoger informaciones de organizaciones sociales: http://www.indymedia.org/es/

655 Foro social mundial en castellano: http://www.forumsocialmundial.org.br/index.php?cd_language=4&id_menu=

656 Castells, M. *La era de la información: economía, sociedad y cultura (Vol. 1): La sociedad red*. Alianza editorial. Madrid. 2008

657 . De nodo 50 ya hemos tratado en anteriores ocasiones, al ser el principal valedor de medios alternativos en España: http://www.nodo50.org/

el gran agregador de medios de información alternativa sin ánimo de lucro para todo tipo de ONG y organizaciones alternativas españolas (1211 hacen uso de sus servicios actualmente). Pangea[658], con un carácter menos combativo y un cariz más orientado a las ONG de servicios, es otro de los servidores a disposición de este tipo de organizaciones. Otro de los referentes de medios alternativos para España y Latinoamérica, surgido en 1996, prácticamente en paralelo a la confluencia de organizaciones antes descrita, será Rebelión[659], que se alimenta de informaciones múltiples y artículos de grandes firmas como Noam Chomsky o James Petras, habiendo sido capaz de establecer una red de colaboradores voluntarios que mantienen una capacidad de información crítica diaria con una visión alternativa a la de los medios comerciales, libre y múltiple que deja en manos del lector los instrumentos para analizar e interpretar las noticias.

El siguiente paso, lo dará una nueva generación de organizaciones, todavía más vinculadas a la red. Entre estas, se producirá un proceso de confluencia global. Como hemos ido desgranado a lo largo de los anteriores capítulos, nuevas formas de respuesta ciudadana se organizan desde y hacia la red, para interpretar y dar respuesta a la configuración del propio sistema en torno a Internet.

---

[658] 14. http://www.pangea.org/

[659] Rebelión ha sido el mayor agregador de contenidos de información alternativa en la red en lengua castellana. Su longevidad y la información que recoge lo hace uno de los referentes en la comunicación al margen de los medios tradicionales. Destaca especialmente, los artículos de opinion de firmas como N. Chomsky o J. Petras: www.rebelion.org

Ya hemos tratado de varias ramas de activismo cívico y de las plataformas en la red. El primero de estos surgirá de la defensa del software libre, con Stallman y la FSF como los elementos más destacados. En paralelo, la lucha por la revisión de las legislaciones de derechos de autor, y la defensa de nuevas formas de compartir cultura, que interesadamente legisladores y empresas quieren situar en la dicotomía de lo comercial o lo pirata, aparecerán, con Laurence Leesing entre sus figuras destacadas. Con posterioridad, el hacking tomará opción por la acción directa en la oleada de ataques y acciones de propaganda encabezadas por grupos como Anonymous. Estas acciones son simultáneas en el tiempo con las revelaciones primero de WikiLeaks y posteriormente del gran caudal de información directa filtrada por Edward Snowden[660]. Junto a este proceso, entidades de der4chos enfocadas a la red de redes, sobre todo al calor de asuntos como la neutralidad en la red y las negociaciones de tratados restrictivos tanto de libertades como de derechos, como ACTA, como al mayor exponente, se organizaran con la red como principal escenario. Entre las entidades destacadas en el asunto la EFF, merece una mención especial. Como vemos, Organizaciones no gubernamentales, colectivos cívicos y hactivistas de diversa índole han coincidido en articular respectas comunes frente a los grandes temas que han acompañado a la red desde su gestación. Sin el papel activo del estos movimientos y su capacidad de tejer redes y dar a conocer cuestiones sobre las que una prensa ordinaria identificada con el poder no habría no habría aportado luz, viviríamos en una red más restringida hoy en día. Efectivamente, esto ha significado un proceso de confluencia entre un activismo parcial y un progresivo proceso de politización de sectores vinculados a ONG y organizaciones cívicas. El camino hacia una reflexión cada vez más de conjunto de las situaciones, articuladas desde las bases de estas organizaciones ha conseguido que

[660] Greenwald, G. *Snowden. Sin un lugar donde esconderse*. Ediciones B. Barcelona. 2014

comience a articularse procesos de confluencia internacional en torno a propuestas que cada vez más van conformándose hacia una argumentario común y sistematizado[661].

La progresiva politización de sus actores principales, será un paso consecuente en este itinerario. Así la pertenencia de Stallman al partido verde norteamericano, donde colaboraría con la campaña de Ralph Nader o el reciente Anuncio de Laurence Lessing de concurrir en la campaña por las presidenciales de 2016 en EEUU, con el fin de establecer un cambio definitivo en las leyes del copyright, mediante una campaña de crowfounding para no vincularse con lobbies y grandes corporaciones, está teniendo una gran repercusión entre medios de internet al ser uno de los artífices de las licencias *Creative Commons* y uno de los más activos defensores del fin de los derechos de autor tal y como se definen hoy en día[662].

En España, el caso de Pablo Soto es un ejemplo claro de este proceso. Juzgado y perseguido por programar y suministrar diversas herramientas para compartir archivos, con una demanda por parte de *Warner, Universal, EMI, SONY BMG y PROMUSICAE*, este pionero en las tecnologías *P2P* finalmente sería declarado inocente al no lucrase ni establecer negocio alguno en la copia no reconocida legalmente[663]. En

---

661 Lanier, J. *Contra el rebaño digital: Un manifiesto*. Debate. Barcelona. 2011

662 El anuncio de Leesing sobre su concurrencia a las elecciones presidenciales de 2016 en EEUU es una noticia muy reciente: http://www.eldiario.es/cultura/fenomenos/Lawrence-Lessig-convertirse-presidente-dejarlo_0_419258330.html

663 El abogado de Soto, David Bravo, otro activista por los derechos en Internet y sobre la propiedad intelectual daría cuenta de las intenciones del juicio: Ihttp://www.filmica.com/david_bravo/archivos/007844.html . En su obra, *"Copia este libro*", detalla la estrategia de estas multinacionales que se ajusta al caso: http://elastico.net/archives/005194.html

España, esto significará un cambio definitivo en la estrategia de las discográficas de persecución de tecnologías y usuarios, para ir integrándose en plataformas como el *Streaming*. Soto, colaboraría con el movimiento del 15 M., especialmente en Madrid. El siguiente paso sería concurrir en las elecciones municipales de mayo de 2015 en la candidatura de Ahora Madrid, como independiente, sin adscripción partidaria[664].

El movimiento 15M, que recibe el nombre de la primera convocatoria de protesta el 15 de mayo de 2011, sería uno de los ejemplos en los que red y calle confluyen en el comienzo de una articulación de respuesta política y social frente al sistema y sus maneras [665]. El movimiento adquirirá una rápida politización mientras se mantenía estrictamente al margen de formaciones parlamentarias. Muchas de las acciones derivarían en la formación de diversas plataformas de convergencia como las mareas en defensa de diversos servicios públicos, derechos cívicos u otras organizaciones finalistas como la Plataforma de afectados por la Hipoteca (PAH), que jugará un papel fundamental en la visualización de los procesos de desahucios llevados a cabo por las entidades bancarias a partir de la crisis de 2008 con unas acciones que tendrán gran eco mediático, especialmente en los bloqueos a ejecuciones de desahucio[666] .

---

[664] Las sucesivas victorias de Pablo Soto a las discográficas en las demandas a su aplicaciones de búsqueda y descarga P2P sentarían un precedente en lo que respecta a los límites legales de la ofensiva de las grandes compañías del medio contra usuarios: http://www.genbeta.com/actualidad/pablo-soto-vuelve-a-derrotar-a-las-discograficas-crear-y-difundir-redes-p2p-en-espana-es-legal

[665] . El propio movimiento establecerá unos mecanismos a través de los que ofrecer comunicación en las redes como la denominada *15MPedia,* con información y orientaciones a los activistas y participantes*: http://15mpedia.org/wiki/15M*

[666] La Plataforma de Afectados por la Hipoteca, es una de las organizaciones más activas en lo que va de década, tanto porel carácter de sus acciones como por su reivindicación

La teorización de la hipótesis de los "seis grados de separación", inserta en las redes sociales, puede visualizarse en las comunicaciones sociales en torno al 15M de manera muy gráfica[667]. La interrelación entre usuarios de redes sociales y la difusión de lemas y eventos entre sus seguidores tendrán un efecto exponencial. Las nuevas formas de analítica nos permiten conocer el modo en que esta expansión se difunde entre las redes de cada usuario y cómo salta a través de esta para extenderse con un alcance generalizado. Precisamente la descentralización y el salto entre nodos, con la capacidad de cada uno de extender los mensajes, será una de las claves para comprender la rápida expansión del movimiento y la simpatía generalizada que alcanzaría en sectores mayoritarios de la población, la que muchos llamaron la *#spanishrevolution* y que sería precedente de una oleada mundial de manifestaciones con puntos de partida similares[668]. La relevancia de ciertos usuarios de redes como Facebook y Twitter en la difusión de *#hashtags* (etiquetas que identifican una idea a modo de consigna), poseerán por si mismas un efecto multiplicador en la difusión de las ideas y principios del movimiento. La simpatía generalizada de personajes y usuarios muy vinculados a las redes será capaz de crear un impacto a escala.

---

propiamente dicha.: http://afectadosporlahipoteca.com/

667 La hipótesis de los seis grados de separación, creada por el escritor húngaro Frigyes Karinthy en un cuento llamado *Chains*. Trata de explicarnos que cualquier persona puede estar conectado a cualquier otra a través de una cadena de conocidos que no tiene más de cinco intermediarios, lo que uniría a ambas personas mediante seis enlaces. La idea, es empleada de forma recurrente al tratar de explicar las redes sociales y el alcance de los mensajes.

668 . Un análisis sobre las formas de organización y empleo de las redes por parte del 15M, muy interesante podemos encontrarlo en*: DatAnalysis15M: Evolución del sistema-red 15m a través de la topología de redes*: *http://www.slideshare.net/elaragon/dat-analysis15m*

La propia campaña para las presidenciales del entonces candidato Barak Obama será uno de los ejemplos de uso de la redes junto con un conocimiento del impacto de cada intervención y una analítica de Big Data hasta entonces desconocida en lo que respecta al empleo de herramientas provenientes de la web para su empleo en una campaña política. El éxito de la campaña residiría en la capacidad de movilizar a buena parte del electorado que se inhibía de otras convocatorias y una medición bastante precisa de los aspectos más relevantes para ofrecer contraste y focalizar el voto. El impacto entre sociólogos y analistas de las nuevas formas de comunicación de esta campaña hará que su análisis haya adquirido una gran relevancia en nuestros días[669].

En España, la desproporcionada reacción contra la protesta ha derivado en la comúnmente llamada *Ley mordaza* (Ley de Seguridad Ciudadana), que desde julio de 2015 incluye sanciones a formas de protesta derivadas del 15M. Así, grabar a un policía, elemento fundamental en la condena de abusos, o la resistencia pacífica, otra de las maneras de permanecer en espacios públicos, tiene cuantiosas sanciones e incluso penas de cárcel. La conciencia de la dimensión de este movimiento y su eventual politización en torno a candidaturas populares, junto con la visualización constante de actividades contra desahucios o los escraches, especialmente frente a casos de corrupción, ha provocado una reacción desproporcionada, que difícilmente concuerda con un estado de derecho y que diarios como El New York Times calificarái en su editorial como "ominosa"[670]. Diversas ONG e incluso el grupo de derechos humanos de la ONU, exigen su retirada, al encotrar su redacción lesiva a cierto número de

---

669 . Seoane, F. *Activismo Político en la era digital: El empleo de Internet para el compromiso político en las convocatorias web*. Capítulo de: VVAA. Cultura digital y movimientos sociales. Catarata. Madrid. 2008

670 El duro editorial del diario Neoyorkino va en sintonía con el documento que hacía mención a las consecuencias de la crisis en España y la pone en relación con las medidas de austeridad: http://www.nytimes.com/2015/04/23/opinion/spains-ominous-gag-law.html

derechos fundamentales, lo que coloca a España en cuestiones relativas a estos derechos fundalentales en un foco donde hacía décadas que no se ebncotraba[671].

Este proceso de confluencia entre nuevas formas de organizarse y una protesta contra la estructura de poder establecida y el cuestionamiento de los métodos y formas en las que la ciudadanía se relaciona con este poder tendrá una influencia muy importante a escala global. Así movimientos como Ocuppy, (surgido a partir de una primera protesta contra el poder de Wall Street, en EEUU[672] o Yosoy132, en México, significarán un nuevo referente en los movimientos sociales que volverán a ser masivos y contestatarios tras un largo periodo de dominio incontestado del pensamiento único y la alternancia.

Como hemos visto, la identificación de diversos agentes del conflicto en la red con ideologías y zonas de interés e influencia son un proceso natural en la formación de bloques políticos. El interés por establecer una alternativa a la hegemonía de los elementos del sistema a través de alternativas de cambio desde las bases del mayor interés ciudadano será el paso consecuente con este proceso. La certeza de que la mayor parte de estados y empresas ya tienen una pertenecía clara a un modelo ideológico no hace más que abundar en las fuentes del conflicto. Una tensión descrita en la dialéctica más clásica y que vuelve a definirse en el nuevo contexto de la red de redes[673].

---

[671] La noticia sobre los redactores de la ONU frente a la denominada Ley de Seguridad Ciudadana, tendrá un importunarte eco mediático en el mes de abril de 2015. Como ejemplo el diario.es: http://www.eldiario.es/politica/ONU-Codigo-Penal-Mordaza-Espana_0_359764361.html

[672] La web del movimiento Norteamericano Ocuppy: http://www.occupy.com/

[673] AAVV. *¿Quién vigila al vigilante?* Un Informe de Privacy internacional disponible en: https://www.privacyinternational.org/?q=node/351

Las llamadas *Primaveras Árabes*, aunque que resulte complejo unificar todo el proceso de revueltas en países musulmanes de la ribera mediterránea y oriente próximo en una sola categoría, han sido otro de los referentes en los que la función de la comunicación social llegaría a tener un papel fundamental en el cambio social. Aunque unificar en una sola denominación a la serie de protestas, revueltas y levantamientos acontecidos en varios países del Magreb y oriente próximo desde 2010, sería arriesgado, más allá de los efectos de influencia y coincidencia temporal, muchos de los movimientos sí que coincidirían con las formas en las que las protestas ciudadanas estaban sucediendo en otros lugares del mundo[674]. Así aunque con un resultado desigual, las protestas en Túnez o Egipto, lograrían derrocar a los gobiernos, mientras en Libia o Siria, desembocarían en guerras civiles en el que movimientos de corte yihadista aprovecharían la situación para hacerse con territorios y recursos. Túnez sería el primero de estos estados donde se producirían una serie de protestas que en cierto modo recordaran en sus inicios a movimientos como los del 15 M. Jóvenes desempleados y sin perspectivas de futuro, se lanzan a protestar por la situación en la que viven. La espontaneidad del movimiento, potenciado por la capacidad de comunicación a través de Internet, será uno de los factores que más se destacará y que será común en buena parte de los movimientos que se extiendan por otros territorios, especialmente Egipto[675]. La censura y el intento de bloquear Internet, servirá para que buena parte de la comunidad más concienciada de la red ofrezca formas de conexión alternativas a los manifestantes egipcios. Así,

---

674 La primavera Árabe vista por Eric Hobsbawn, uno de sus últimos documentos: http://www.bbc.com/mundo/noticias/2011/12/111229_primavera_arabe_hobsbawn_revolucion_pea.shtml

675 Samir Amin haría una crónica sobre la situación económica y social que empujaría a la situación de Egipto y el resultado final de todo el proceso. http://rebelion.org/noticia.php?id=129400

Twitter y Facebook, podría seguir manteniendo su servicio en una red censurada por Mubarak a través, por ejemplo, de la plataforma Acess Now, que permitía la existencia de nodos de conexión con Egipto de la red Tor mediante los que poder evitar el filtrado y censura de medios[676]. El cierre completo de Internet por parte de un gobierno egipcio cada vez más inestable, no pudo parar la movilización y las noticias pudieron seguir saliendo al exterior por otros medios. Una de las lecciones de este proceso, en el apartado de la permanencia de las redes sociales más allá de los intentos de cierre y censura, será que la capacidad de la población de encontrar medios de sortear la censura supera en este momento las formas en las que esta puede aplicarse[677].

Si la censura en la red es un indicador de la calidad democrática de las naciones, Turquía, a pesar del apoyo occidental a este estado laico en manos de un gobierno de un islamismo con aspiraciones de ser visualizado como "asimilable", tampoco saldría bien parada en todo este proceso[678]. Las manifestaciones de 2013 iniciaran un proceso de censura y persecución. La propia obsesión del presidente Erdongan contra las redes sociales y especialmente Twitter, al que acusaba de ser *"la peor amenaza para la sociedad"* y el encarcelamiento de periodistas y activistas en el ejercicio de la libre expresión han conseguido cuestionar seriamente la legitimidad de su gobierno. El cambio de DNS (servidores que dan salida a la red) y posteriormente tan solo la canalización de la red a través de redes VPN (que cifran los datos hacia un servidor externo) han podido

---

[676] El acceso a la red donde exista censura, se convertiría en una de las bases de muchas OGN durante la llamada Primavera Árabe. *Acces Now* será de las primeras en ofrecer formas de acceder hacia la red: https://www.accessnow.org/

[677] Sobre el cierre definitivo de Internet en Egipto. Enrique Dans redactaría en su blog una crónica bastante detallada: http://www.enriquedans.com/2011/02/como-se-apaga-internet-en-todo-un-pais.html

[678] Los mapas de *Open Net* nos muestran los niveles de censura y filtrado de Internet en el mundo. Para el caso egipcio, puede consultarse el histórico: http://map.opennet.net/

conseguir eludir la censura del gobierno turco. Los últimos capítulos a lo largo de 2014, directamente relacionados con la corrupción que salpicaría al mismo gobierno, han llevado a que tanto la legislación que permite la censura como el bloqueo a medios como YouTube o Vimeo por mantener contenidos de denuncia, puedan seguir su labor y la población tenga que seguir empleando técnicas de elusión para informarse[679] [680].

Por último y más reciente aún, el caso de las protestas en Hong Kong nos harían ver la dificultad que una censura de medios tecnológicos tiene hoy en día. El despliegue de la red a través de las propias antenas de los terminales de los manifestantes nos apunta a una madurez y sofisticación progresiva de los medios de eludir la censura. La llamada protesta de los paraguas, por el uso masivo de este accesorio por parte de los manifestantes frente a los botes de gases, a lo largo de septiembre y octubre de 2014, pondría el foco en la manera en la que la confluencia de los "dos sistemas" en China, se concretaría en las futuras elecciones del 2017 en Hog Kong. El gobierno chino, una vez integrado en su territorio Hong Kong, anunciaría el método de presentación de candidaturas a las elecciones locales de la ex colonia en la que unos criterios particulares filtrarán de hecho la libre concurrencia. Por otro lado, el programa educativo chino, implantado desde la unificación y acusado de dogmatismo, provocaría una movilización en sectores estudiantiles. La confluencia del movimiento estudiantil y la movilización por unas elecciones democráticas derivaran en una oleada de protestas. La exigencia de grupos identificados con los sectores más jóvenes de la población de la excolonia para pedir una democratización en China y en Hong Kong más

---

679 VVAA. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), ISBN 0-262-51435-4 http://www.access-controlled.net

680 Informe de la UNESCO sobre la censura de internet Titulado: *Freedom of Connection, Freedom of Expression,* disponible en: Freedom of Connection, Freedom of Expression

concretamente, conseguirán una visualización a escala internacional en parte por su capacidad de comunicación y por la focalización de medios exteriores a cualquier acontecimiento social en China[681].

Joshua Wong, uno de los activistas en la manifestación más reconocido del movimiento, animaría a través de su perfil de Facebook a que los manifestantes se instalaran y emplearan la aplicación *Firechat* en sus terminales móviles. EN 24 horas, más de 100.000 personas habían descargado la aplicación, de los desarrolladores de Open Garden. Una de las características de esta aplicación de mensajería es su capacidad, si las redes de datos de las operadoras se encuentran caídas, como sucedía en Hong Kong, o se hace uso de inhibidores de señal por parte de la policía o se restringen las antenas de telefonía, es que puede cambiar la forma de conectarse a través de las antenas Wifi o Bluetooth, saltando el mensaje en forma de red en malla entre los usuarios conectados De hecho, la propia afluencia masiva de personas que se conectan a un mismo sistema de antenas puede desbordar la capacidad de estas, como se puede comprobar en cualquier concentración medianamente nutrida a la que asistamos. Así, la sola existencia de otros usuarios con la aplicación, crear una infraestructura en red mediante la cual los mensajes puedan difundirse sin depender de otro medio que del propio terminal. Esta forma de comunicación, sería esencial en estas manifestaciones, al establecer un método alternativo de transmisión de mensajes fuera de la capacidad de restricción[682]. Así, más allá de la repercusión del movimiento en sí, será el

---

[681] Como en muchas ocasiones en temas recientes y de impacto periodístico, Wikipedia puede ofrecernos una de la mejor síntesis de los hechos: https://es.wikipedia.org/wiki/Protestas_en_Hong_Kong_de_2014

[682] Sobre el uso de *Firechat*, se escribiría profusamente al convertirse en la herramienta fundamental del movimiento en Hong Kong: http://www.bbc.com/mundo/noticias/2014/09/140930_tecnologia_hong_kong_app_protestas_ig

indicador de cómo las nuevas formas de comunicación pueden imponerse a medios restrictivos lo que destaca en el enfoque de nuestro estudio. De nuevo las formas de eludir censura y bloqueo a la comunicación vuelven a imponerse[683].

Lo casos de censura en la red se han ido multiplicando en proporción a su propia extensión. En general, la capacidad de la población de comunicarse en libertad, sin ser conducida por unos medios afines, son siempre observadas con recelo. La capacidad de que la censura, el bloqueo o la dificultación del acceso tengan resultado depende de factores como el nivel sociocultural de la población y la propia extensión del uso de Internet. La universalización de este, complica cualquier intento de bloqueo completo e incluso el filtrado se dificulta. Como veremos, uno de los primeros grupos en ampliar sus conocimientos en la gestión de las redes y la censura, serán los grupos activistas y los periodistas. Al ser su labor una de las primeras víctimas de cualquier cierre o censura de redes, han sabido madurar a lo largo de todos los procesos de estos últimos años para poder establecer contramedidas muy eficaces. Casos de cierre completo como el de Egipto, son medidas extremas y desesperadas que usualmente no optaría ningún gobierno y por tanto, la mera existencia de cierta capacidad de conexión, puede bastar para encontrar un cauce de salida[684].

La censura no solo afecta a momentos puntuales de actividad de masas o revueltas populares. Circunstancias mucho más usuales como la censura de Facebook en Irán, que sin embargo cuenta con unos 19 millones de usuarios, no hacen más que demostrarnos cómo las aspiraciones de la población supera la censura. El uso de Proxys y VPN,

---

683 En lo que respecta a empleo de medios tecnológicos para la difusión y explicando el empleo de *Firechat*, *The Atlantic* hizo una muy buena síntesis en su monento: http://www.theatlantic.com/technology/archive/2014/10/firechat-the-hong-kong-protest-tool-aims-to-connect-the-next-billion/381113/

684 . Para saber si una web es bloqueada en cierto país, existe una pasarela que nos permite comprobarlos directamente: http://www.blockediniran.com/

como veremos en el último capítulo, permiten de forma relativamente sencilla, poder recuperar el acceso a estas redes. El caso es tan solo la anécdota de una censura y una posterior estrategia de vigilancia de las redes, en las que los medios alternativos se hacen un lugar cada vez más destacado[685].

Redes sociales. Propietarios y usuarios.

El auge de las redes sociales y su popularización, especialmente a partir del momento en el que al acceso a la red se ha hecho móvil y por tanto permanente e instantáneo, ha supuesto un cambio en la forma de establecer cauces de comunicación entre personas y colectivos. En ello, los medios clásicos, televisión generalista y prensa escrita, no han sabido adaptarse con la suficiente velocidad y nuevas formas de tendencia horizontal se han abierto camino a través de estas redes. En todo este proceso, el fenómeno de la blogsfera, la publicación independiente y los canales específicos de comunicación, como por ejemplo los de vídeo, con YouTube como principal valedor, han supuesto las bases de las que partirán los usuarios para compartir contenidos entre su red de contactos. Como hemos visto, la capacidad de las redes sociales se ha manifestado especialmente a lo largo de la segunda década de nuestro siglo. La extensión a lo largo de toda la población y el uso intensivo de herramientas de comunicación, han llevado a un momento en el que estas redes han adquirido una importancia fundamental para el ejercicio del poder y el

685 Informe de Reporteros Sin Fronteras. *"Enemigos de Internet 2014: organismos en el epicentro de la censura y la vigilancia*": http://www.rsf-es.org/news/rsf-publica-el-informe-enemigos-de-internet-2014/

establecimiento de una hegemonía social que comienza a ser menos unívoca[686].

El flujo de datos y la comunicación social en la red es una realidad que en nuestros días mueve cifras millonarias. La penetración de Internet llega a 3.010.000 personas, el 42% de la población mundial. Tan solo las cuentas en redes sociales a través de dispositivos móviles alcanzan los 1.685.000 usuarios, lo que significa una penetración del 23% de la población del planeta. El uso de dispositivos móviles ya ha superado el 51% de la población, con cifras de crecimiento interanuales de un 23%. Las cifras, aplicadas a estados más desarrollados, especialmente Europa, Estados Unidos y Asía, arrojan cifras muy superiores, que en la práctica supone una extensión casi completa de las redes y en la generalización de los usos sociales. En concreto tanto Europa como El norte de América[687], superan ya el 80% de la población que hace uso de Internet[688].

La penetración del uso del móvil amplía sus bases en dos extremos, por un lado los países en los que la extensión generalizada y la mejora de los caudales de ancho de banda progresan más rápido y por otro entre naciones menos desarrolladas, cuya adopción de internet está directamente siendo vía dispositivos móviles, como puede ser el caso de Nigeria[689].

---

686 . UIT: (Unión internacional de Telecomunicaciones- ITU en inglés) datos sobre la penetración de internet en el mundo en el periodo 2000-2015 https://www.itu.int/net/pressoffice/press_releases/2015/17-es.aspx

687 . El informe de la agencia *We Are Social* sobre el impacto del intercambio de información y las comunicaciones a través de redes sociales 2015 nos ubica en la realidad de las redes sociales en nuestro tiempo: http://wearesocial.sg/blog/2015/01/digital-social-mobile-2015

688 . UIT: Porcentajes de uso individual de Internet por países http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

689 Estudio de Nielsen sobre el uso del

En España existen 50 millones de conexiones móviles, lo que supera a la población y una conexión social mediante estos dispositivos que alcanza al 38% de la población, cifra que asciende al 47% si no discriminamos dispositivos, mientras los usuarios activos de internet ya superan el 77%. Los principales servicios los encabeza WhatsApp, con una penetración del 42%, seguida de Facebook y su mensajería, con un 33% y Twitter con un 17%, seguidas de otras redes sociales y servicios de mensajería que no superna el 10%. Para hacernos un idea de la dimensión que la movilidad ha representado en el aumento del uso de las redes sociales, la media de tiempo empleado en acceder a diversos servicios de internet vía móvil es de 1 hora y 51 minutos, tiempo que iguala el uso de redes sociales en general y que está ya próximo a las 3horas 31 minutos que se suele emplear en la televisión en promedio[690].

Las cifras de usuarios de las diversas rede sociales también apuntan a la masiva entrada de nuevos. Facebook, con 1.366.000 usuarios registrados, es la red hegemónica en todo el planeta. Le siguen servicios de mensajería como WhatsApp o WheChat, muy implantado en Asia, o Skype, y redes sociales como Twitter, con 560 millones de cuentas e Instagram, con 150 millones. El caso de Google+ es algo excepcional, dado que es la puerta de acceso a muchos de los servicios de Google, como las cuentas en dispositivos Android, e incluso durante un tiempo a YouTube, por lo que la red de la gran G, ofrecía cifras de usuarios que entraban en disonancia con la actividad de la red en cuestión. Una práctica

---

Smartphone: http://www.nielsen.com/us/en/insights/news/2015/so-many-apps-so-much-more-time-for-entertainment.html

690 . UIT: (Unión internacional de Telecomunicaciones- ITU en inglés) datos sobre la penetración de internet en el mundo en el periodo 2000-2015 https://www.itu.int/net/pressoffice/press_releases/2015/17-es.aspx

fallida, que finalmente, a lo largo de 2015 ha abandonado la empresa y está demostrando el fracaso de su propuesta de red social[691] [692].

Como vemos, para la gran empresa, poder apuntar hacia las redes sociales es una de las claves de la disputa por la hegemonía del tráfico de usuarios. La red se ha convertido en una pasarela por la que multitud de usuarios emplean las redes sociales como medio general. La estrategia de integración, seguida por Facebook, que recordemos que es propietaria tanto de Instagram como de WhatsApp, puede derivar en tráficos millonarios que se traducen directamente en cifras de negocio. Por ello, no nos debe extrañar que redes como Facebook, estén integrando noticias o vídeos dentro de su propio sistema, para convertirlo en una especie de portal personal en la que la clave está en el tiempo de permanencia máximo de sus usuarios[693].

La cuestión más significativa, al analizar la extensión de las redes sociales a través de la población mundial es acerca de qué redes son las que encuentran mayor implantación y quien es su propietario. La mayor crítica a esta extensión de los usos sociales viene precisamente del análisis de sus propietarios y la dirección que estas, como negocio, tienen. Efectivamente, podemos decir que la práctica totalidad de las redes sociales o las plataformas que hacen uso de funciones sociales pertenecer a empresas privadas radicadas en Norteamérica y sujetas, por

---

[691] Op. Cit. 690.

[692] La propia CIA, mantiene unas bases de datos estadísticas sobre el uso mundial de Internet muy intersantes. https://www.cia.gov/library/publications/the-world-factbook/rankorder/2153rank.html

[693] La EFF haría un estudio sobre qué datos personales recopila y cómo los maneja cada una de estas empresas. Así como la forma de proceder respecto a la protección de estos o la cesión a peticiones de gobiernos y jueces: https://www.eff.org/who-has-your-back-government-data-requests-2015

tanto al derecho de su país. Legislaciones como las europeas han tratado de matizar el hecho de que los datos se encuentren fuera de Europa con legislaciones como la de la directiva de protección de datos, que luego tendría sus desarrollos locales en cada estado de la UE, como es el caso español[694].

La toma de conciencia de este hecho, todavía no se ha consolidado en nuestros días entre los usuarios de Internet. Incluso tras las publicaciones de los informes de transparencia que tanto Facebook, como Google o Twitter publican anualmente y que hacen referencia clara a las peticiones de diversos estados e instancias judiciales sobre datos de sus usuarios, se han conseguido establecer cauces paralelos generalizados para la conexión social vía Internet[695] . La acomodación de la ciudadanía hacia unas redes ya conocidas, nos ha llevado a un momento donde la dependencia hacia un restringido grupo de empresas de todas las comunicaciones sociales es absoluta.

Los sucesivos escándalos en torno a la facilidad de intervención de WhatsApp y su falta de cifrado, algo solventado a primeros de 2015, junto

---

[694] La Directiva sobre la Protección de datos de carácter personal de la UE (95/46/EC) trata de paliar las carencias jurisdiccionales de asuntos como los datos en las redes sociales:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[695] Los informes de transparencia de las tres grandes empresas propietarias de redes sociales, pueden servirnos como un claro indicador de cómo está evolucionando la política de infrmación al respecto y cómo las grandes de la red tratan de salvaguardar su imagen tras los sucesivos escándalos de filtraciones y cesiones de datos:

- Google: https://www.google.com/transparencyreport/?hl=es
- Facebook: https://govtrequests.facebook.com/
- Twitter: https://transparency.twitter.com/

con el anuncio de su compra por parte de Facebook, haría que grupos de usuarios con mayor conciencia de la privacidad se pasaran a usar otras redes como Telegram, que permite el cifrado de comunicaciones y no requiere conocer datos personales para hacer uso de ella. Intentos más ambiciosos de sustitución, como el Caso de Diáspora, por citar uno de los que más repercusión conseguirían, apenas movilizaría a un número limitado de usuarios en los primeros estados de su creación. Así, la realidad actual es que la expansión y el predominio de las redes sociales en tiempos de uso y número de personas que hacen uso de internet, no para aumentar su base, mientras las garantías de privacidad, tanto la declarada como en un valor más profundo de compromiso con la libertad frente a casos como los de espionaje, no están del todo claras (52).

Por otra parte, que la generalidad de las redes sociales pertenezca a empresas privadas significa que si su uso es gratuito para los usuarios, el peaje que estos hacen es convertirse por sí mismos en parte del negocio. Así alimentar el Big Data de estas grandes compañías, junto con el consumo publicitario debidamente orientado, son partes fundamentales de estas redes y la orientación principal de estas (53). El desconocimiento de estas prácticas y la disimulada ocultación de estas por parte de las empresas propietarias, ha conseguido crear una atmósfera de libertad irreal en torno a estas redes. Sucesivas campañas de grupos activistas por las libertades en la red han hecho hincapié en la indefensión de una ciudadanía que hace cesión de sus datos de forma poco meditada o sin conocimiento real de la dimensión que estos datos adquieren dentro de la red. A pesar de ello, hechos como la capacidad de ejercer nuestro derecho al olvido tendrán escasa repercusión en una red donde los datos pueden ser replicados al instante.

Con este panorama, la adopción de nuevas formas de comunicación horizontal de la ciudadanía, sobre todo en las cuestiones

más vinculadas al activismo y el compromiso político, se ven en la actualidad frente a una situación limitante. Los nuevos movimientos sociales que giran en torno a organizaciones horizontales de ciudadanos, que algunos denominan democracia liquida y se articulan en torno a portales y medios de comunicación basados en la red , con el Smartphone como instrumento básico, cada vez más extendido, se enfrentan a una realidad limitante respecto a la soberanía respecto al medio. Son muchos los casos de cierres o suspensiones de cuentas de usuarios en Twitter o Facebook, frente a los que existe una indefensión frente a la que no se han articulado alternativas. La dependencia de las redes sociales más extendidas de parte del activismo cívico es uno de los mayores problemas a los que puede enfrentarse en las democracias occidentales, dado que están expuestas al arbitrio de unas políticas de uso fijadas por compañías norteamericanas.

La red extensa. Hashtags, Memes y efecto Streisand

Hemos visto como las redes sociales se han extendido y como son un instrumento político y social de primer orden. Pero las redes sociales no cumplen ese objetivo como función prioritaria. Las redes se han convertido, especialmente en la seguida década del presente siglo en una forma de comunicación extensa. Atrás queda el momento en el que la especialización de las redes y foros respondía a cierto nivel sociocultural de sus integrantes (54).

El uso banal de las redes, es otra de las consecuencias de su extensión y la intención de abarcar a un público cada vez mayor. Esta popularización de la red también ha producido cambios en las formas de interactuar en las redes entre colectivos generalistas. El que redes sociales como Twitter se hayan convertido en fenómenos *mainstream* (generalista)

ha tenido un impacto directo incluso entre medios tradicionales. Así en la lucha por las horas centrales de las parrillas televisivas, el uso de etiquetas y la movilización de espectadores vía redes sociales es un fenómeno muy común, especialmente en espectáculos de tipo Reality Shows (55). El fenómeno del ruido social ha ido en paralelo a la implementación de herramientas para segmentar públicos e intereses, dado que las redes mismas son las primeras interesadas en que no se desincentiven sus usuarios (56).

Con el tiempo, la red ha conseguido imponer su lenguaje particular y extenderlo al resto de los canales de comunicación. Multitud de cuestiones surgidas de una forma u otra a partir de los usos propios de las redes han terminado por considerarse cuestiones de la cultura popular de nuestro tiempo.

Los *memes*, son un fenómeno acuñado por el genetista Richard Dawkins, en su libro el Gen Egoísta, para describir los procesos de pervivencia intelectual de ciertas formas de transmisión cultural. En este sentido, pudo asimilar ciertas pautas de evolución y transmisión de información en unidades informacionales que denominaría meme (derivado de la mímesis), en comparación con el propio gen, como contenedor de información (57). El éxito de ciertas publicaciones, sobre todo en los comienzos de YouTube, irán asociados al término meme. .Años después, la red comenzaría a usar el término en referencia a bromas y chistes que se repetían y difundían entre ciertas comunidades hasta llegar a constituir un lenguaje propio. El foro libre 4Chan, será uno de los referentes en este sentido. Creado por el entonces adolescente Christopher Poole, inspirándose en los foros japoneses dedicados a la manga, pasaría pronto a convertirse en una referencia, por su capacidad de anonimato y su completa libertad de contenidos, especialmente entre internautas de lengua inglesa. Como ya explicamos el termino Anonymous

nace de este foro, ya que es el nombre por defecto de todas las cuentas que escriban en los diversos hilos que componen el foro. De la multiplicidad de bloques temáticos, el que más relevancia obtendrá será /b/ "randon", el foro de temática libre. Navegar por sus hilos puede ser un ejercicio complejo para alguien profano a las practicas del colectivo, muy dado a las autoreferencias y a empleo masivo de memes que si se desconocen pueden desorientarnos (58).

El uso del término Meme suele ir de la mano del de "viral", aunque este último caso ha sido muy empleado en campañas comerciales. En principio, la *viralidad* hacía referencia al éxito y extensión rápida de ciertas publicaciones en la red. Especialmente vídeo de YouTube en sus orígenes. Poco después, la capacidad de extensión sería adoptada por publicistas y supuestos gurús del medio digital para campañas comerciales hasta extenderse por otros medios como la televisión.

Con el tiempo Twitter, por su naturaleza asimétrica y la capacidad de compartir contenidos acompañada de la concreción que su límite de 140 caracteres impone, se convertirá en todo un referente en cuanto a la información inmediata. Entre los medios de comunicación, periodistas e informadores, será un medio por el que compartir enlaces y datos rápidamente. Precisamente su concisión, hará que el etiquetado de publicaciones sea muy usado desde sus orígenes. Así el denominado Hashtag (el símbolo # seguido de la palabra elegida), será la forma de seguir un hilo concreto de ciertas informaciones, con una repercusión que llevará a otras redes sociales a adoptarlo como propio. En las redes sociales es otra de las cuestiones más comúnmente empleadas.

El llamado efecto Streisand es otro de los fenómenos surgidos de las redes sociales que hoy en día son tomados en consideración a la hora

de tratar de censurar u ocultar una información. En efecto en cuestión, tiene su origen en el intento de la Actriz norteamericana Bárbara Streisand de que se retirara una foto de su lujosa propiedad en la costa californiana, que aparecía en una publicidad. La amenaza de demanda al fotógrafo, de una información intrascendente en origen, popularizaría la imagen en internet y terminó por focalizar más aún la polémica (59). En esencia, se trata del efecto contrario al deseado que se produce al intentar coartar o censurar ciertas informaciones. Casos como el secuestro de la revista El Jueves por su parodia de la monarquía española o como las publicaciones de la revista francesa *Charlie Hebdo,* serán ejemplos de popularización de imágenes de este tipo.

La extensión de la red y en concreto de las formas de comunicación sociales ha supuesto la oportunidad en nuestros tiempos de una nueva manera de extensión social, de la cada vez más difícil extensión de la censura y el control de la información. Por otra parte, esta extensión adolece de dos males radicales. Por una parte, las redes sociales mayoritarias pertenecen a empresas privadas a cuyo arbitrio están estas sometidas, aunque el principal interés sea el comercial, como ya hemos señalado (60). Por otro lado la banalización y el peligro del *clictivismo*, la concreción del compromiso social no más allá de unos golpes de ratón, es una amenaza real a los movimientos sociales que pueden caer en un efecto de laxitud en la actividad que los deje como meros difusores de información. Esta amenaza de dilución del compromiso y de adocenamiento por la vía comercial, vuelve a poner en la balanza la dicotomía entre los ciudadanos y los consumidores, si la sociedad será capaz de tomar los nuevos instrumentos para dirigir el cambio social o seguirá las pautas dirigidas desde la pantalla de sus terminales de última generación (61).

NOTAS

1. Ugarte de, D. El poder de las redes. Colección Biblioteca de las Indias. Madrid. 2011

2. VVAA. Pásalo. Relatos y análisis sobre el 11M y los días que siguieron. Traficantes de sueños. Madrid. 2014

3. EL informe de David de Ugarte, titulado, "11M: Redes para ganar una guerra", también analiza el impacto de las comunicaciones alternativas a los medios tradicionales: www.lasindias.com/informes/11m.pdf

4. Castells, M. Comunicación y poder. Alianza Editorial. Madrid. 2009.

5. Sánchez de Almeida, C. República Internet. Un libro en formato Blog (hasta julio de 2013) http://republicainternet.com/

6. Assange, J. Cypherpunks. La libertad y el futuro de internet. Deusto. Madrid. 2014.

7. VVAA. Internet y Lucha política: Los movimientos sociales en la red. Capital Intelectual, Buenos Aires, 2006

8. Ramonet, I. Pensamiento único y nuevos amos del mundo. Icaria. Barcelona. 2008

9. http://www.attac.org/

10. http://www.indymedia.org/es/

11. Foro social mundial en castellano: http://www.forumsocialmundial.org.br/index.php?cd_language=4&id_menu=

12. Castells, M. La era de la información: economía, sociedad y cultura (Vol. 1): La sociedad red. Alianza editorial. Madrid. 2008

13. De nodo 50 ya hemos tratado en anteriores ocasiones, al ser el principal valedor de medios alternativos en España: http://www.nodo50.org/

14. http://www.pangea.org/

15. rebelión ha sido el mayor agregador de contenidos de información alternativa en la red en lengua castellana. Su longevidad y la información que recoge lo hace uno de los referentes en la comunicación al margen de los medios tradicionales: www.rebelion.org

16. Greenwald, Glenn - Snowden. Sin un lugar donde esconderse. Ediciones B. Barcelona. 2014

17. *Lanier, J. Contra el rebaño digital: Un manifiesto. Debate. Barcelona. 2011*

18. *El anuncio de Leesing sobre su concurrencia al as elecciones presidenciales de 2016 en EEUU es una noticia muy reciente:* http://www.eldiario.es/cultura/fenomenos/Lawrence-Lessig-convertirse-presidente-dejarlo_0_419258330.html

19. EL abogado de Soto, David Bravo, otro activista por los derechos en Internet y sobre la propiedad intelectual daría cuenta de las intenciones del juicio: lhttp://www.filmica.com/david_bravo/archivos/007844.html . En su obra, "Copia este libro", detalla la estrategia de estas multinacionales que se ajusta al caso: http://elastico.net/archives/005194.html

20.. Las sucesivas victorias de Pablo Soto a las discográficas en las demandas a su aplicaciones de búsqueda y descarga P2P sentarían un precedente en lo que respecta a los límites legales de la ofensiva de las

grandes compañías del medio contra usuarios: http://www.genbeta.com/actualidad/pablo-soto-vuelve-a-derrotar-a-las-discograficas-crear-y-difundir-redes-p2p-en-espana-es-legal

21. EL propio movimiento establecerá unos medios a través de los que ofrecer comunicación en las redes como la 15MPedia. Con información y orientaciones a los activistas y participantes*: http://15mpedia.org/wiki/15M*

22. La Plataforma de Afectados por la Hipoteca, es una de las organizaciones más activas de lo que va de década tanto por sus acciones como por su reivindicación.: http://afectadosporlahipoteca.com/

23. La hipótesis de los seis grados de separación, creada por el escritor húngaro Frigyes Karinthy en un cuento llamado *Chains*. Trata de explicarnos que cualquier persona puede estar conectado a cualquier otra a través de una cadena de conocidos que no tiene más de cinco intermediarios, lo que uniría a ambas personas mediante seis enlaces. La idea, es empleada de forma recurrente al tratar de explicar las redes sociales y el alcance de los mensajes.

24. Un análisis sobre las formas de organización y empleo de las redes por parte del 15M, muy interesante podemos encontrarlo en: DatAnalysis15M: Evolución del sistema-red 15m a través de la topología de redes: *http://www.slideshare.net/elaragon/dat-analysis15m*

25. Seoane, F. Activismo Político en la era digital: El empleo de Internet para el compromiso político en las convocatorias web. Capítulo de: VVAA. Cultura digital y movimientos sociales. Catarata. Madrid. 2008

26. El duro editorial del diario Neoyorkino va en sintonía con el documento que hacía mención a las consecuencias de la crisis en España y la pone en relación con las medidas de austeridad: http://www.nytimes.com/2015/04/23/opinion/spains-ominous-gag-law.html

27. La noticia sobre los redactores de la ONU frente a la denominada Ley de Seguridad Ciudadana, tendrá un importunarte eco mediático en el mes de abril de 2015. Como ejemplo el diario.es: http://www.eldiario.es/politica/ONU-Codigo-Penal-Mordaza-Espana_0_359764361.html

28. La web del movimiento Norteamericano Ocuppy: http://www.occupy.com/

29. ¿Quién vigila al vigilante? Informe de Privacy internacional disponible en: https://www.privacyinternational.org/?q=node/351

30. La primavera Árabe vista por Eric Hobsbawn, uno de sus últimos documentos: http://www.bbc.com/mundo/noticias/2011/12/111229_primavera_arabe_hobsbawn_revolucion_pea.shtml

31. Samir Amin haría una crónica sobre la situación económica y social que empujaría a la situación de Egipto y el resultado final de todo el proceso. http://rebelion.org/noticia.php?id=129400

32. El acceso a la red donde exista censura, se convertiría en una de las bases de muchas OGN durante la llamada Primavera Árabe. *Acces Now* será de las primeras en ofrecer formas de acceder hacia la red: https://www.accessnow.org/

33. Sobre el cierre definitivo de Internet en Egipto. Enrique Dans redactaría en su blog una crónica bastante detallada: http://www.enriquedans.com/2011/02/como-se-apaga-internet-en-todo-un-pais.html

34. Los mapas de *Open Net* nos muestran los niveles de censura y filtrado de Internet en el mundo. Para el caso egipcio, puede consultarse el histórico: http://map.opennet.net/

35. VVAA. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), ISBN 0-262-51435-4 http://www.access-controlled.net

36. Informe de la UNESCO sobre la censura de internet. Freedom of Connection, Freedom of Expression, disponible en: Freedom of Connection, Freedom of Expression".

37. Como en muchas ocasiones en temas recientes y de impacto periodístico, Wikipedia puede ofrecernos una de la mejor síntesis de los hechos: https://es.wikipedia.org/wiki/Protestas_en_Hong_Kong_de_2014

38. Sobre el uso de *Firechat*, se escribiría profusamente al convertirse en la herramienta fundamental del movimiento en Hong Kong: http://www.bbc.com/mundo/noticias/2014/09/140930_tecnologia_hong_kong_app_protestas_ig

39. EN lo que respecta a empleo de medios tecnológicos para la difusión y explicando el empleo de Firechat, The Atlantic hizo una muy buena síntesis en su monento: http://www.theatlantic.com/technology/archive/2014/10/firechat-the-hong-kong-protest-tool-aims-to-connect-the-next-billion/381113/

40. Para saber si una web es bloqueada en cierto país, existe una pasarela que nos permite comprobarlos directamente: http://www.blockediniran.com/

41. Informe de Reporteros Sin Fronteras. "Enemigos de Internet 2014: organismos en el epicentro de la censura y la vigilancia": http://www.rsf-es.org/news/rsf-publica-el-informe-enemigos-de-internet-2014/

42. UIT: (Unión internacional de Telecomunicaciones- ITU en inglés) datos sobre la penetración de internet en el mundo en el periodo 2000-2015 https://www.itu.int/net/pressoffice/press_releases/2015/17-es.aspx

43. El informe de la agencia *We Are Social* sobre el impacto del intercambio de información y las comunicaciones a través de redes sociales 2015 nos ubica en la realidad de las redes sociales en nuestro tiempo: http://wearesocial.sg/blog/2015/01/digital-social-mobile-2015/

44. UIT: Porcentajes de uso individual de Internet por países http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

45. Estudio de Nielsen sobre el uso del Smartphone: http://www.nielsen.com/us/en/insights/news/2015/so-many-apps-so-much-more-time-for-entertainment.html

46. Óp... cit. 42

47. Óp. cit. 43

48. La propia CIA, mantiene unas bases de datos estadísticas sobre el uso mundial de Internet muy intersantes. https://www.cia.gov/library/publications/the-world-factbook/rankorder/2153rank.html

49. La EFF haría un estudio sobre qué datos personales recopila y cómo los maneja cada una de estas empresas. Así como la forma de proceder respecto a la protección de estos o la cesión a peticiones de gobiernos y jueces: https://www.eff.org/who-has-your-back-government-data-requests-2015

50. La Directiva sobre la Protección de datos de carácter personal de la UE trata de paliar las carencias jurisdiccionales de asuntos como los datos en las redes sociales. (95/46/EC)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

51. Informes de transparencia de las tres grandes empresas propietarias de redes sociales:

- Google: https://www.google.com/transparencyreport/?hl=es
- Facebook: https://govtrequests.facebook.com/
- Twitter: https://transparency.twitter.com/

52. Campañas como la de *Naked Citizens* (ciudadanos desnudos) hacen hincapié precisamente a la exposición no solo a la vigilancia sino a la completa confección de perfiles personales con los que cuentan las compañías de internet hoy en día: https://www.nakedcitizens.eu/

53. Reclaim your data es otra de las campañas llevadas adelante en la UE por activistas de la red para que la ciudadanía ejerza sus derechos sobre los datos que tienen las diversas empresas: http://www.reclaimyourdata.eu/

54. Cobo, C. y Pardo H. Planeta Web 2.0. Inteligencia colectivao medios fast food. Grup de Recerca d'Interaccions Digitals, Universitat de Vic. Flacso México. Barcelona / México DF. ,2007 (con licencia CC disponible en http://www.planetaweb2.net/)

5. VV.AA. Sociedad Mediatizada. Gedisa. Barcelona.2007

56. Gillmor, D. Nosotros el medio. 2004. Libro disponible con licencia Creative Commons en: http://www.hypergene.net/wemedia/espanol.php

57. Resultan curiosas las reflexiones de Dawkins, años después de la teorización sobre los memes, al ver cómo tanto el termino como su uso se ha extendido en la red en: Dawkins, R. El capellán del diablo. Gedisa. Barcelona. 2005.

58. En el documental "Somos Legión La Historia de los Hactivistas", se explica, por boca de muchos de sus protagonistas, como desde las

bromas de 4Chan surgirán las primeras campañas de Anonymous: https://www.youtube.com/watch?v=ee19z6D1yxo.

59. Dans, E. Todo va a cambiar. Deusto. Madrid. 2010

60. Jones, O. Chavs. La demonización de la clase obrera. Capitán Swing. Madrid. 2012

61. Lanier, J. Contra el rebaño digital: Un manifiesto. Debate. Barcelona. 2011

4.5 Moneda virtual y las nuevas vías del negocio delictivo global.

Atender a las fuentes del mercado delictivo global en nuestros días y su evolución sería un estudio que transcendería el ámbito del presente trabajo. El énfasis de nuestro trabajo va especialmente enfocado a cómo la red a servido como plataforma de cambio en las formas de organización de diversos colectivos, entre el que el delictivo es uno de los más rápidamente adaptables. Así, negocios ilegales como el del tráfico de drogas, las formas de pago ocultas y el incremento de las ventas por la red, ha permitido que este tipo de negocios apunten hacia la red como forma de exponer sus productos. Como hemos señalado, el negocio delictivo se ajusta mejor que ningún otro al paradigma del modelo capitalista ideal. Con ello, la existencia de una demanda, al margen de aspectos legales, es rápidamente cubierta por un mercado que surge alrededor de ella. El auge de la red en todos los aspectos de nuestra vida cotidiana, supone, siguiendo esta misma lógica que tanto productos ilegales como delitos se adapten a las nuevas formas de comunicación.

Por otro lado, la aparición de las denominadas *criptomonedas*, dinero generado en la red, reconocido por toda la comunidad de usuarios y

por tanto convertible a moneda habitual y forma de pago extendida, ha supuesto otro punto de inflexión en el establecimiento de nuevos paradigmas. Todavía el impacto de la nueva situación que supone el uso de este tipo de monedas está asentándose y extendiéndose, aunque su cada vez mayor aceptación apunta hacia un futuro en el que el sistema monetario actual, fruto de los acuerdos que abandonarían el patrón oro a cambio de la flotabilidad de las monedas y el sistema actual de mercados financieros, donde el valor especulativo condiciona la economía real (1).

Las redes criminales tienen una influencia capital en la economía de ciertas naciones, y la adecuación de su forma de actuación al modelo de la red como lo hemos descrito en capítulos anteriores es un paso lógico por tanto. La Mafia siciliana, Yakuzas japonenses, Cárteles colombianos y mejicanos, Triadas chinas y las redes criminales rusas, son todas ellas organizaciones asentadas con una ingente capacidad de movilización de capitales e influencia, dedicados desde hace décadas al tráfico de drogas, armas, trata de blanca, inmigración ilegal o blanqueo de dinero, entre sus actividades más destacadas. La adaptación del negocio a las nuevas formas y la estructura de redes era, por tanto un proceso previsible entre este tipo de organizaciones (2). La integración de nuevas formas de delincuencia en este tipo de redes y la inevitable persecución de quienes mantienen negocios en el mismo territorio son fuentes habituales del conflicto. Como ejemplo, el supuesto asesinato del *spammer* ruso Alexey Tolstokozhev responsable del 30% del correo basura, especialmente dedicado a la venta de viagra, en 2007, sería una señal de la forma en la que unas organizaciones delictivas en su fases maduras actúan contra agentes independientes en su medio (3). Más allá de la certeza que tengamos acerca del caso, el interés está en las nuevas formas de organizarse del delito tecnológico y el proceso de maduración e integración en mafias preestablecidas en otros ámbitos. Un proceso por otro lado de esperar, en cuanto a que este tipo de organizaciones no toleran negocios paralelos ni competencia en sus “ámbitos de actuación”.

Podemos afirmar que el negocio delictivo global, ha sido uno de los que mejor han sabido integrarse en las nuevas formas de una economía que tiene en internet uno de sus pilares organizativos fundamentales. Con ello, veremos que la asunción de una moneda ubicada en la red y de difícil rastreo o el establecimiento de canales directos de venta y distribución a través de formas ocultas de difundir su mercancía convertirá a la red en el lugar ideal para abrir nuevos mercados.

La criptomoneda como ejemplo de un nuevo paradigma

En una sociedad en la que el modelo especulativo de la banca de inversión y la búsqueda de beneficios no vinculados a una economía real está en pleno apogeo, incluso a pesar de sr consecuencia directa de la crisis iniciada en 2008, la aparición de las denominadas criptomonedas sería acogida de forma desigual. . Mientras que ciertos sectores especulativos verían en ello un refugio estable ante fluctuaciones, la evolución de sus precios y varios procesos de inestabilidad llevarían a que monedas como el Bitcoin, la moneda virtual más conocida, hayan pasado por varias situaciones extremas aunque su valor general, desde sus inicios no haya dejado de incrementarse (4).

Sobre la atribución del Bitcoin se sabe poco aunque se especulado largamente. El nombre de Satoshi Nakamoto, pseudónimo del creador o colectivo de creadores, ha sido la única referencia que se tiene con certeza. A lo largo de estos años y pesar de las muchas atribuciones, algunas documentadas, se desconoce la identidad de su creador. Los intercambios de comentarios en los foros de la P2P Foundation, tampoco aclararían el asunto salvo el desmentido de una de las últimas atribuciones. De cualquier modo, la moneda, de código abierto (adaptando la licencia MIT), verá la luz en 2009 y pronto comenzará a ser adaptado por

plataformas en red y como medio de pago en muchos servicios de la red (5).

La idea de las monedas virtuales, o criptomonedas, parte de un concepto totalmente vinculado al proceso matemático de la creación de archivos únicos, identificables y verificables por luna comunidad de poseedores de otras monedas. Su valor parte de un proceso de producción constante pero limitado en el que una progresiva disminución de la cantidad nueva de moneda generada cada año acompaña a una dificultad creciente en lo que respecta a su creación. De este modo, en 2009, era posible crear Bitcoins con un ordenador convencional haciendo uso de la GPU (tarjeta gráfica). Apenas un año después tan solo mediante dispositivos especializados o servidores especialmente orientados a los motores gráficos se podía generar la moneda de forma rentable. En poco tiempo, la creación de esta monda escaparía a la posibilidad de cualquier usuario convencional. Así surgirían comunidades que compartían ancho de banda de sus conexiones para obtener crédito en la generación colectiva de la moneda. Estos grupos pasarían después al alquiler de infraestructuras de servidores dedicados por empresas ya dedicadas a tal fin, dado que el nivel de complejidad alcanzado a finales del 2012 dejaba atrás cualquier intento viable en cuanto a gasto eléctrico e inversión en hardware. La producción de esta moneda sigue un proceso decreciente en el que la confluencia de mineros y la frecuencia de generación de moneda seguirá un proceso invertido en el que se ira estabilizando en un modelo de cada vez menor producción. Con este parámetro, resultaría en principio más fácil conocer el número global de esta moneda existente y poder establecer su precio de conversión con la moneda convencional (6).

La masiva inversión en Bitcoin de los años 2013-2014 llevaría a unas cotizaciones que alcanzarán los 1000 dólares el Bitcoin. De esas cifras, se ha llegado a un 2015 en el que la moneda ha permanecido en torno a los

200 dólares. Mucha responsabilidad de este fenómeno lo ha tenido tanto la inversión masiva de especuladores como sucesivos casos de caídas de grandes empresas dedicadas al cambio y venta de esta moneda. En 2013, la empresa de capital riesgo Andreessen Horowitz, se haría con una cartera de 25 millones de dólares. Apenas un mes más tarde *Blockchain*, el mayor gestor de carteras de esta moneda, afirmaba contar con un millón de estas y *Coinbase*, otra gestora de carteras, con 650.000. Un año después se produce el primer gran desplome de la moneda, asociado al cierre de *Silk Road*, el denominado supermercado de la droga en Internet, que contaba en las carteras de sus gestores con una ingente cantidad de esta moneda, junto con la caída en bancarrota de *MtGox*, el principal cambista de la moneda que supondría la pérdida de 650.000 Bitcoins (7). Este desplome, también ha supuesto un freno en la creación de servidores dedicados a la minería de esta moneda, que ahora deben reajustar sus criterios de rentabilidad a la nueva realidad de la moneda. De cualquier modo, tras el auge especulador y la posterior caída, el precio general de la moneda sigue siendo muy superior al de partida y si marginamos este proceso, sigue en aumento. Las magnitudes de los últimos años llevarán a autoridades como la británica a establecer una serie de consejos de forma oficial sobre los riesgos de este tipo de monedas (8).

El futuro de este tipo de intercambios se prevé imparable a tenor de varios factores. Una moneda que facilita los pagos inmediatos, multidisposivo (lo que en el móvil resulta destacado), segura, a pesar de los varios ataques a carteras famosas, que no revela la identidad del propietario y que no cobra comisiones, por ejemplo permitiendo envíos de dinero fuera de los establecimientos bancarios clásicos, es una moneda que apunta al futuro y que está aún en proceso de maduración (9) a pesar de no ser reconocida por las autoridades monetarias en la actualidad.

Bitcoin no es la única criptomoneda en el mercado actualmente. En el último quinquenio se han creado más de un centenar de este tipo de monedas con diversas cualidades particulares. Una profusión de monedas que puede consultarse en sitios como *Coinwarz*, que recoge la cotización de casi un centenar de distintos modelos. Se estima que el proceso de confluencia irá en paralelo a la maduración de estas, sobre todo teniendo en cuenta que en su mayor parte se tratan de proyectos abiertos y distribuidos que parten de un código fuente consultable (10). En torno a esta moneda se han creado una serie de negocios de cambio y cotización que resultan similares a los de la banca ordinaria y que permiten simplificar el uso y se prevé que la paulatina integración, cuando las legislaciones nacionales comiencen a reconocer su uso y expansión, será un hecho. Recientes cambios como el implementado en la forma de crear Bitcoin con el llamado Bitcoin XT, una actualización de la moneda para poder acelerar su proceso de transacción y reconocimiento y que abre el debato a propósito de los límites de adaptación de una moneda de este tipo para acondicionarse a la evolución de su mercado (11). Esta adaptación, es precisamente una de las capacidades que permite una moneda de código abierto, que no tiene propietario ni gestor único y que parte del ideario P2P.

Bitcoin es vista por muchos como la oportunidad para cambiar el orden de la economía y las finanzas, fijado de manera tendenciosa por los poderes económicos. Una oportunidad de fijar una moneda que escapa completamente a mecanismos de control. La realidad nos dirá hasta qué punto una moneda puede pivotar en un cambio de paradigma económico y social sin ser sometida al control de los actores principales.

Las fuentes del negocio oculto y el mercado ilegal

Aunque la difusión de spam, (correos basura no deseados y de origen sospechoso) sería durante los primeros años de la expansión de la red uno de los pilares de la venta ilegal, con el establecimiento de las primeras BotNets (redes de ordenadores infestados para ser controlados por el spammer), el crecimiento de métodos restrictivos y el control de los tráficos han llegado a desincentivar esta vía de negocio. Hoy en día, la mayor parte del spam que pervive está más vinculado al uso no consentido de listas de usuarios por parte de campañas publicitarias y directamente a la estafa.

El siguiente estado de maduración del negocio de venta de productos ilegales será el de la ocultación de la identidad y el pago también oculto. Veremos cómo la unión de una criptomoneda en expansión junto con la entrada en una red oculta, hasta entonces territorio de activistas, expertos y aficionados a diversos géneros pornográficos, entre sus usuarios más habituales, dará una nueva dimensión al negocio de la venta ilegal *(12).*

Unas de las atribuciones más comunes a la *Deep Web* y la *Dark* W*eb* es la de la existencia de sitios dedicados a cuestiones ilegales, pornografía infantil, venta de armas y drogas. También suele ser un lugar común, hasta el hastío, la descripción de la *Deepweb*, la web profunda, como la parte sumergida de un gran iceberg, en el que los usuarios "normales " apenas somos conscientes de la parte más superficial. La realidad de la red es algo diferente a todas estas ideas precocinadas. Si bien es cierto que existe una gran parte, mayoritaria, del tráfico del Internet más convencional que ocurre de forma no transparente para los usuarios, esto no significa ninguna ocultación de datos. Buena parte de los intercambios de información de la red se producen entre máquinas y servicios específicos, que circulan de forma cifrada, de redes privadas, sobre todo en entornos empresariales , o simplemente de correos

electrónicos de los que tan solo tenemos acceso, por supuesto, a nuestras propias cuentas. Con esta idea, reconoceremos que al tratar de la web no debemos simplificar así como tampoco deberíamos buscar complejidades y zonas oscuras donde lo existen (13).

Actualmente existe tres grandes redes ocultas, que permiten la navegación prácticamente anónima, siempre que el usuario las emplee correctamente, que son TOR (The Onion Router), que es la red más famosa (14), I2P, una red privada que también cuenta con cierta extensión (15) y FreeNet, que se sostiene como una red P2P (16). La primera es la más famosa y empleada actualmente de forma mayoritaria. En ciertos entornos de censura, la opción por la navegación siempre cifrada comienza a contemplarse como la única opción viable para la ciudadanía, como veremos en el capítulo siguiente. Con ello, la expansión de este tipo de redes es un proceso incremental que sigue en nuestros días.

Esta capacidad de ocultación atrae cada vez a sectores más amplios de la población y a servicios antes ubicados en la red convencional. Así el caso de The Pirate Bay, el mayor *tracker* (contenedor de enlaces) de *torrents* y enlaces *magnet* (la forma derivada y distribuida del *torrent*), mantiene su web en la red TOR mientras su página en la web convencional sigue una suerte de azares por los que suele cambiar de ubicación con frecuencia (17). Asimismo, suministran una versión del navegador de TOR especialmente adaptado a la búsqueda de archivos torrents para la descarga, llamado The Pirate Browser (18). Con ello, se cierra el círculo del acceso y la descarga en países donde esta es perseguida, tanto por operadoras como por gobiernos, dado que tanto la obtención de los enlaces como su posterior descarga, con clientes torrents capaces de ofuscar la conexión, puede ser ocultado al completo. Algunos foros, especialmente de intercambio de archivos o especialmente preocupados por la privacidad de sus usuarios han migrado a estas redes.

Legislaciones que penalizan los enlaces, han propiciado este movimiento. Otras páginas como Deep Dot Web, que se dedica a informar sobre la Deep Web mantiene replicada su web convencional con otra en la red de TOR. Como vemos, hay muchas motivaciones por las que servicios no directamente vinculados al entorno delictivo pueden querer migrar a servicios ocultos (19). Las motivaciones adquieren cada vez un rango más variado.

El acceso a estos servicios de redes ocultas, que en lugar de las extensiones clásicas que nuestros navegadores aceptan tales como *HTML, Asp o PHP* entre las más comunes, suelen tener una extensión denominada *.Onion.* Para tener acceso a estas hay que contar con un navegador capaz de interpretarlas y un acceso a estas redes. La tarea se ha simplificado mucho desde que se extendiera el uso de navegadores embebidos en los que todo el acceso está pre configurado, como el caso del famoso *TorBumble*, que no es más que un Firefox con las configuraciones de TOR precargadas, que está disponible en la web de la propia página de la fundación (20).

De cualquier modo, la vinculación del elemento criminal y el tráfico de mercancías ilegales y la web ha sido un elemento recurrente a lo largo de prácticamente toda la extensión de internet. La posibilidad de establecer foros privados o ejemplos todavía más ocultos a través de redes de anonimato como la red TOR ha permitido que negocios de este tipo puedan funcionar. La combinación de estos servicios que otorgan anonimato junto con el cobro en criptomoneda ha permitido que unas nuevas formas de negocio delictivo puedan conformarse en la red (21)

La puerta de entrada a estos servicios, desde un navegador es algo diferente. En cierta medida se parece a la primera web en la que no todo estaba a golpe de buscador y había que acceder mediante portales o intermediarios a ciertas partes de la red o conocer la *url* (dirección) concreta. En TOR, lo usual es empezar desde *The Hidden Wiki*, una especie de portal que compendia enlaces catalogados según lo que busquemos (22). El buscados de referencia en la web oculta es *Torch*, con 88.804 páginas tipo *.Onion* listadas en su base de datos (23). Más recientemente, el buscador *Grams*, una especie de Google de la red oculta, ha comenzado a rastrear y listar páginas, de forma análoga a como lo hacen los robots de google (maquinas que rastran la web para proporcionar resultados de búsquedas). La especialización de Grams son las tiendas de la red oculta. Así, ahora mismo es fácil poder encortar páginas y establecer cauces de confianza en las compras ilegales, dado que emplea criterios ya conocidos en la web transparente (24).

La clave en este tipo de mercados negros, al igual que mercados transparentes, como el ejemplo de eBay, reside en la confianza ente el pagador y los que hacen uso de sus servicios. La mayor parte de estas tiendas, en esencia portales de compraventa, mantienen un sistema de puntuación que permite al posible comprador saber la reputación de quien le ofrece su producto y así poder tomar su decisión de compra con la confianza de compras anteriores.

Los recientes ataques por parte agencias policiales, a varias de las páginas como *Silk Road* antes a *Black Market*, tan solo han conseguido que otras puedan emerger o que réplicas de estas sean de nuevo puestas en marcha. El mercado negro de mercancías ilegales en la red, es uno de los negocios de este tipo que mayores beneficios reporta a sus propietarios con una inversión en tiempo, recursos e incluso riesgos que ningún otro negocio de este tipo en el mundo físico puede tener. Las cifras de este

mercado, que pueden mover unos 450.000 € al día, fundamentalmente en criptomoneda, nos da una idea del alcance del fenómeno. Estudios como el de *Usenix* (publicado en agosto de 2015), sobre los mercados negros en las redes anónimas, apuntan a que los productos que mayor demandan movilizan son los productos farmacéuticos tipo Viagra y OxyContin, seguidos de drogas como la Marihuana y el MDMA. La mayoría de los mercados de este tipo ven que sus mayores ventas se enfocan en este sector, a pesar de lo vistoso que nos resulta ver la venta de armas u otros elementos turbios. Las cifras del negocio, se estiman en torno a una horquilla de los 100-180 millones de dólares anuales y por tanto nos explican el porqué de que los cierres recurrentes no hagan más que aflorar nuevas páginas (25).

El siguiente paso, en una red en la que no hay garantías, es el establecimiento de confianza entre comprador y vendernos. Esto se realiza mediante dos prácticas bien definidas. En primer lugar el *Escrow*, que es la retención por parte del intermediario, en este caso el portal de ventas, del dinero hasta la confirmación de la transacción (26). Con ello se ofrece una relativa garantía al comprador de que este vendedor cumple con su negocio, aparte del sistema de puntuación que estas mismas páginas tienen. Por otro lado, en caso de pretender que los Bitcoins en cuestión no puedan ser identificados individualmente, existen unos intermediarios que se dedican a la remezcla de estos. Así entidades dedicadas a la mezcla de criptomonedas, como *BitMixer*, aceptan el depósito del comprador y pagan al vendedor con otra moneda distinta de su depósito particular, asegurando así la imposibilidad de que la transacción pueda ser rastreada (27).

Por supuesto, que exista un negocio oculto no quiere decir que el acceso tenga que ser complejo. Para poder colocar adecuadamente productos ilegales como drogas, armas o vulnerabilidades de sistemas, hay que poder mantener unos servicios que no puedan ser rastrados pero por

otra parte fácilmente accesibles. En este sentido, los mercados negros han evolucionado de forma rápida, desde las páginas convencionales hacia la migración de sus servicios a redes ocultas. Para facilitar la tarea, se mantiene puentes entre la web convencional y la oculta o se dispone de buscadores específicos para acceder a las partes más ocultas de la red. La publicidad de estos entre sectores interesados en la compra es una de las fuentes del spam actual, tal y como indicábamos.

Delitos y cibercrimen en la era digital

Conocidos lo métodos de ocultación y la forma de pago, el panorama del delito en la red se cierra con las formas en las que los ciber delincuentes atacan y se hacen con datos ajenos. Actualmente, la cantidad de datos personales que circulan por la red y la cada vez mayor integración de nuestra vida corriente en el entorno digital hace que seamos más vulnerables al acceso o robo de datos. El mercado de hacking y sus formas ilícitas es algo que vive un momento de expansión en nuestros días. Como hemos ido viendo en capítulos anteriores, la ampliación de la base de usuarios con conocimientos avanzados sobre la red y su seguridad, junto con un momento en el que la crisis económica ha cerrado muchas vías de empleo y precarizado sectores enteros, ha podido propiciar que un mercado negro de los servicios delictivos en la red se vea incentivado por tales circunstancias (28). En ese sentido, el caso ruso ha sido uno de los ejemplos paradigmáticos pero, como veremos, tanto China como América latina, son otras fuentes en las que se expande este tipo de negocios. Las formas de explotación de vulnerabilidades de sistemas y la capacidad de intrusión en estas es algo de lo que se viene documentando desde los años noventa del pasado siglo. La actitud de los hackers de aquellos momentos distaba algo de lo que podemos ver hoy en día. En los primeros tiempos el desafía o una forma de activismo hacker era la vía común de ataques, junto con el *crack* de programas comerciales y videojuegos (romper la protección

anti copia). En España, sería la protesta frente a telefónica de grupos como *Hispahack*, sobre la posición abusiva de la compañía y las limitaciones que el práctico monopolio del momento imponía, terminaría en juicio y posterior absolución, por falta de pruebas en 1999. Los llamados defacement (cambio de la página de sitios por otras con lemas de protesta) sería una de las practicas que también serían perseguidas. Hasta 2010, el hacking no sería delito según el código penal español, momento en el que la profesionalización del medio y la distinción entre White Hat y Black Hat (sombreros blancos o negros según orientaran su labor a la seguridad o al delito) comenzará a conformar la realidad actual (29).

La capacidad de conocer a través de herramientas OSINT (open Source Inteligence), cada vez mayor número de datos personales, muchos de ellos cedidos voluntariamente por parte de los usuarios de redes sociales, nos permite ser cada vez más certeros en la búsqueda de información para un posterior ataque (30). El propio navegador Google, contiene herramientas avanzadas, denominadas *dorks* que nos permiten establecer rastreos de servicios a personas y empresas para determinar ciertos elementos de sus redes por las que poder probar vulnerabilidades. Todo ello unido a otras herramientas más avanzadas como *Shodan*, conocida como el buscador de los Hacker y otras como *Maltego* o *FOCA*, nos pueden permitir, sin una gran inversión en conocimientos, aproximarnos a una recolección de datos muy grande (31). En muchos casos, a esta fase de recolección de datos sigue otra de acceso a las maquinas encontradas y la búsquedas de vulnerabilidades. Hoy en día sigue siendo muy común encontrar maquinas, tanto personales como en entornos profesionales, no actualizadas convenientemente (32). La publicación diaria de bases de datos tipo CVE (de fallos de sistema que pueden ser explotados) junto con métodos cada vez más estandarizados de utilización de estas fallas en los sistemas, como el caso del reconocido *Metasploit* (un entorno de trabajo para la gestión de vulnerabilidades en equipos), han permitido que el ataque a infraestructuras se convierta en un

proceso de escasa complicación para hackers de conocimientos medios (33). Las posibilidades de intrusión en sistemas que pueden ser secuestrados, espiados o puestos en uso de forma externa nos dan un abanico extenso de opciones delictivas.

Ejemplos como el *Carding*, la venta de tarjetas de crédito clonadas o sustraídas por diversos métodos a través de la red oculta, es un práctica muy corriente y su posterior venta en mercados negros, como los que hemos descrito más arriba, se mantiene de forma permanente (34). Otros casos muy comunes en nuestros días son los *APT*, ataques persistentes dirigidos contra una sola víctima, en las que se deduce un interés especial por acceso a sistemas y que correctamente enfocados solo sistemas bien fortalecidos pueden evitar en la actualidad. El avance de este tipo de ataques viene acompañado de otro tipo de intervenciones de equipos todavía más claramente enfocada a la extorsión. El *Ransonware* (traducido del inglés como software de secuestro), es un tipo de intrusión en sistemas que cifra todos los datos personales del usuario y le emplaza a que pague, en carteras de criptomoneda, para recibir la llave de descifrado de estos (35). Si unimos la falta de políticas de seguridad, junto con la escasa conciencia en lo que respecta a las copias de seguridad de datos críticos, el asalto a ciertos profesionales y empresas puede provocar enormes perjuicios. Incluso pagando, no hay garantías de la restauración de los archivos. Otros casos como los ya mencionados ataques DDoS, la suplantación de identidad o la redirección de páginas web no protegidas hacia réplicas que instalan malware (cualquier tipo de software con fines maliciosos) son muy comunes y extendidas (36).

El aumento de las ciberamenazas y su extensión hacia todo tipo de usuarios de la red son ya un hecho generalizado. Las diversas

conferencias de ciberseguridad que salpican el calendario son esperadas por los entornos de seguridad para conocer las nuevas explotaciones de vulnerabilidades más destacables que diferentes investigadores encuentran. Las *DefCom* de Las Vegas, que se llevan celebrando todos los veranos desde 1992, es una de las citas más esperadas (37). Por poner un ejemplo, el acceso a Chips NFC o la capacidad de intervenir la señal de vehículos eléctricos, junto con la publicación de fallos de seguridad en dispositivos Android e iOs son novedades de su edición de 2015. En España *Rootedcom* es el evento más reconocido al respecto, que agrupa a profesionales de la seguridad y el hacking ético en la presentación de novedades e investigaciones del sector (38).

En lo que respecta a la organización de criminales, Rusia tiene un papel destacado en cuanto a las formas más sofisticadas de empleo del hacking delictivo (39). Informes como el de *Trend Micro*, titulado *Russian Underground,* hace mención a como desde foros en la web convencional, diversos ciberdelincuentes ofrecen servicios de lo más variopinto. El caso de ruso es considerado por entidades de seguridad estatales como uno de los lugares de origen de los mayores ciberdelincuentes de nuestro tiempo (40). La confluencia de un nivel educativo elevado y unos niveles de vida muy limitados hacen que la explotación tecnológica de recursos ajenos sea atractiva. Foros como *antichat.ru, xeka.ru y cardingcc.com*, a apuntan a todo un mercado negro del hacking ilícito, en la mayor parte de los casos ofrecido al mejor postor. Dicho informe, actualizado desde 2004 anualmente, hace un análisis especial sobre el caso de los hackers de este país al ser, junto con China y EEUU una de las naciones que mayor tradición al respecto tienes. El matiz que lo hace especial, es la capacidad de ofrecer la gama más completa de servicios actualmente en conocimiento en lo que respecta a la seguridad. La maduración en las prácticas antiforense de estos colectivos delictivos vuelve a apuntar a los profundos conocimientos de la red y sus medios.

Otros mercados de los servicios más oscuros de la red son América Latina y China. En ambos casos, se pone a disposición del adquirente servicios de hackeo de cuentas de redes sociales, números de tarjetas de crédito, instalación del malware con diversos objetivos. Así se integran toda la variedad delictiva de la falsificación, adaptada al medio tecnológico junto a nuevas formas de spam telefónico y mensajes orientados a la instalación de malware. En algunos aspectos, las operadoras todavía no han aclarado su posición respecto a la venta de servicios de mensajería *Premium*, que siguen aprovechando este tipo de cibercriminales para suscribir a usuarios sin su consentimiento (41). EN este aspecto, hackers chinos llevan años haciendo amplio uso de este vacío. Por otra parte, la instalación de malware dedicado a la obtención de credenciales bancarias es otra de las fuentes principales de este tipo de difusión de archivos orientados a la delincuencia (42). El interés sobre la ciberdelincuencia y la relevancia que está alcanzando recientemente, nos permite conocer mucha documentación acerca de la forma de proceder de estos ataques, especialmente por parte de las empresas de seguridad, muy interesadas en exponer el caso (43) (44).

Según informa la UNODC, (oficina de naciones unidas para las drogas y el crimen), la falta de armonización de las legislaciones nacionales así como la facilidad de operar desde la red por parte de los cibercriminales posibilitaría que este tipo de delitos sigan en aumento. Así en su informa acusa de fragmentación global de la legislación en torno al delito en la red. El avance de las cuestiones dedicadas a la inteligencia y el espionaje no ha ido a la par de una serie de regulaciones en torno a los criterios de seguridad y la forma de actuar frente a la delincuencia en la red (45). Posteriores informaciones podrían darnos una explicación parcial del asunto, al constatar que los procedimientos de control revelados no distaban de los empleados por la ciberdelincuencia. La lectura es bien

clara en este entorno. Si internet ha comenzado a ser empleado como arma contra estados y empresas, delincuentes, ya sean organizados a o a título individual pueden igualmente emplear este tipo de herramientas para establecer procedimientos similares pero que redunden en beneficio propio. En este marco, la capacidad de ocultarse y la falta de colaboración entre estados es la fuente más conveniente para este tipo de actuaciones. Como vimos en los aspectos dedicados a la ciberguerra, la elaboración de esquemas nacionales de seguridad, como el que elabora el Centro Criptológico Nacional, son uno de los pilares básico para organizar una respuesta también al avance de la delincuencia.

Otros casos de hackers, como el conocido *Hacking Team*, nos muestran hasta donde pueden llegar la confluencia de la delincuencia informática y la venta de vulnerabilidades y sistemas de espionaje a gobiernos. Como vimos, finalmente el grupo italiano de hackingTeam también fue infiltrado en sus recursos y la fuga de información respecto a sus contratos y mecanismos pondría en evidencia tanto sus métodos, de ciberdelincuencia, como la ética de sus clientes (47). En esencia, el caso es el de un grupo de ciberdelincuentes que vende sus herramientas a gobiernos, dispuesto a no cuestionar las formas de proceder que eso supone.

Como hemos podido comprobar en esta rápida perspectiva sobre las formas del negocio delictivo de la red, tan adaptado a los patrones que analizáramos respecto a la nueva economía, la explotación de defectos en los servicios y sistemas de la red son una fuente constante de negocio para la delincuencia orientada a esta. Como afirma Víctor Cerf, uno de los creadores de la red, Internet fue creado para que funcionase, incluso en condiciones muy limitadas, no para que fuera seguro. El incremento de servicios, dispositivos y medios de conexión acompañado de la masiva adopción tecnológica de buena parte de la población mundial ha focalizado

en la red a todos los elementos que componen nuestra sociedad. Si bancos, servicios de inteligencia, o medios de comunicación se han adaptado a la nueva plataforma, era de esperar que delincuentes, especialmente con conocimientos avanzados y escasos recursos personales, se enfoquen con dedicación a una red cada vez imbricada en todos los procesos socioeconómicos. Por otro lado, en lo que respecta a la seguridad, criminales espías o terroristas, actúan de formas parecidas en su esquema de ataques a sistemas y por tanto, las defensas que deben preverse tienen que abarcar todos estos aspectos, con independencia de la fuente.

NOTAS

1. Piketty, T. La crisis del capital en el siglo XXI. Crónicas de los años en que el capitalismo se volvió loco. Siglo veintiuno editores. Buenos Aires. 2014.

2. Castells, M. La era de la información: economía, sociedad y cultura (Vol. 3): .Fin del milenio. Alianza editorial. Madrid. 2008

3. Aunque la web *spannhaus*, dedicada al bloqueo de sitios y cuentas que se dedican al envío de correo basura nunca confirmaría estos datos y hay sombras sobre la veracidad del caso, sí que hubo otros casos menos vistosos de asesinato de hackers rusos. http://www.spamhaus.org/

4. La fundación P2P, contiene la mayor parte de los hilos de la creación y puesta en marcha del Bitcoin dentro de sus foros: http://p2pfoundation.net/

5. Después de la creación de la fundación Bitcoin los foros dedicados a la moneda principalmente están en https://bitcointalk.org/

6. Para conocer más sobre la moneda, su propia web de la fundación suministra información sobre cómo se organiza y los medios de compra, generación y gestión de carteras: https://bitcoin.org/es/

7. Sobre el cierre de Silk Road redactaría un artículo en su momento para eldiario.es titulado "El cierre de Silk Road: el gran supermercado de las

drogas de internet": http://www.eldiario.es/turing/Silk-Road-supermercado-drogas-internet_0_183731705.html

8. En marzo de 2015, el gobierno británico publicaría un informe sobre los riesgos de inversión en este tipo de monedas "Digital currencies: response to the call for information": https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf

9. Coinbase es uno de los servicios de cartera e intercambio más estables y empleados en nuestros días:

https://www.coinbase.com/

10. Sobre el mercado de Bitcoin y criptomoneda en cuestión puede consultarse la web de información financiera al efecto Coinwarz:

http://www.coinwarz.com/cryptocurrency/?cal=1

11. Uno de los más recientes cambios en la moneda ha sido la implementación de Bitcoin XT: http://www.ticbeat.com/economia/como-afecta-bitcoin-xt-al-futuro-de-la-criptomoneda/

12. VVAA. *2010 Circumvention Tool Usage Report* (Berkman Center for Internet & Society)

13. Sobre la nueva realidad de la red surgida en la era post Snowden: El fin de la inocencia en la red http://www.eldiario.es/turing/inocencia-red-internet_0_146635468.html y en http://www.rebelion.org/noticia.php?id=170310

14. El proyecto TOR, es la web donde se suministran las herramientas para acceder a la red oculta más famosa de nuestros tiempos: https://www.torproject.org/index.html.en

15. I2P, es otra de las redes que proporcionan privacidad en las conexiones

https://geti2p.net/es/

16. Freenet es la tercera red anónima más utilizada. Especialmente enfocada a foros y comunicaciones entre activistas: https://freenetproject.org/?language=es

17. Por supuesto, sitios como *The Pirate Bay*, mantienen una réplica en TOR, como forma definitiva de eludir la censura y el bloqueo: http://uj3wazyk5u4hnvtk.onion/

18. *Pirate Bay* también cuenta con su propio navegador integrado por el cliente TOR, un Firefox portable y un proxy incrustado: https://piratebrowser.com/

19. Paginas como *Deep Dot Web* también mantienen réplicas de sus webs en la red TOR http://deepdot35wvmeyd5.onion/ y en la web transparente https://www.deepdotweb.com

20. Dos años después de su publicación, en 2013, la Guía *para empezar a usar Tor,* sigue siendo unas grandes fuentes de tráfico, debido al interés despertado por el tema*:* *http://www.eldiario.es/turing/Primeros-pasos-navegacion-segura-Tor_0_126337372.html*

21. Óp. cit. 12

22. The Hidden Wiki, es el portal de acceso desde la web convencional que nos suministra una serie de enlaces a la red oculta. Es conocida como la puerta de entrada más famosa a los servicios ocultos http://thehiddenwiki.org/ . Su versión oculta y sin censura está disponible en: http://zqktlwi4fecvo6ri.onion/

23. Torch, ha sido el buscador de referencia en la web oculta, http://xmh57jrzrnw6insl.onion/

24. Grams, es uno de los buscadores más recientes y que mejores resultados ofrecen en la búsqueda de mercados ilegales en la web oculta. Su funcionamiento, muy parecido al de Google en la web convencional, lo

hace sencillo y fácilmente reconocible en todos sus servicios: http://grams7enufi7jmdl.onion/ . La web Deep Dot Web, hace un análisis bastante convincente de cómo funciona este buscador: https://www.deepdotweb.com/grams-search-darknet-marketplaces/

25. Informe de Usenix sobre la evolución de los mercados negros en la web anónima titulada, *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem:*

https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska.pdf

https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf (actualizado a 11-8-2015)

26. Recopilación de sitios en la web oculta que tiene mercados negros que garantizan la compra mediante Escrow: https://www.deepdotweb.com/marketplace-directory/categories/marketplaces

27. Con Bit Mixer puedes mezclar las cantidades de Bitcoins pagadas a cierto servicio que no quiera ser reconocido. La entidad mezcla con un depósito propio esas cantidades y realiza los pagos con otros Bitcoins de diversos orígenes. De este modo, no solo se hace el pago con una moneda de difícil rastreo sino que este pago queda enturbiado mediante el proceso de mezcla de orígenes:

https://bitmixer.io/how.html

28. Mitnick, K.D. El Arte de la Intrusión. Ra-Ma. Madrid. 2006

29 Molist, M. Hackstory.es. La historia nunca contada del underground hacker en la península ibérica. 2014. Disponible en formato electrónico en: http://hackstory.es/

30. Guía de pasos para la OSINT (tareas de Inteligencia a nivel navegador) para realizar una investigación desde la propia red con los

datos que pueden extraerse de esta sobre individuos y organizaciones. http://onstrat.com/osint/

31. Peña, R. Cuadernos de consultor para el curso de hacking ético. UDIMA. Madrid. 2015

32. VVAA. Pentesting con Kali. 0xwolrd. Madrid. 2014

33. González, P. Metasploit para Pentesters. 0xwolrd. Madrid. 2014

34. El carding, la publicación de datos de tarjetas de crédito para su uso por delincuentes, es una fuente común del negocio del delito en la red: https://www.deepdotweb.com/2015/08/17/cybercrime-the-study-of-carding/

35. Documento informativo a cargo del FBI sobre los ataques y la ciberdelincuencia: *http://www.ic3.gov/media/annualreport/2009_ic3report.pdf*.

36. VVAA. Informe de Amenazas CCN-CERT IA-09/15 Ciberamenazas 2014 y Tendencias 2015. Centro Criptológico Nacional. Madrid. 2015

37. La DefCom las vegas es la conferencia de hacking más reconocida a nivel mundial: https://defcon.org/

38. En España Rootedcom es el evento principal de ciberseguridad y hacking: https://www.rootedcon.com/ , Se pueden consultar los vídeos de las conferencias más destacadas de la edición de 2015 en su canal de YouTube:

https://www.youtube.com/channel/UCeqrsQm33UBFHb50zorReHQ

39. Ponencia sobre Cibercrimen en Rusia: cómo y por qué actúan los ciberdelincuentes en el *I Qurtuba Security Congress:* https://www.youtube.com/watch?v=A0rySsa15nc

40. El informe *Russian Underground* elaborado por TrendMicro en 2012 es uno de los más detallados análisis de cómo se organiza el cibercrimen en el país:

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf . La actualización del informe a Julio de 2015 pone en contraste la rápida evolución del mercado del hacking hacia actividades más específicas como el ataque tipo APT y el Ransonware y la actualización de precios

41. El informe sobre el caso de China tiene sus particulares formas de gestionar el malware con una gran orientación hacia el SMS y el mercado telefonico: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/brazilian-underground-market-for-cybercriminal-wannabes

42. Según TrendMicro, américa latina y especialmente Brasil, comienza a despuntar como un nuevo núcleo de origen de cibercriminales. Así, en su informe sobre la zona, apunta a las formas de adquisición de datos bancarios como una de sus principales focos delinctivos.: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/brazilian-underground-market-for-cybercriminal-wannabes

43. El cuadro completo de informes relativos a los precios y especializaciones del mercado negro y la criminalidad en la red puede consultarse en: http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/

44. Informe anual de la empresa de seguridad Symantec sobre las amenazas para la seguridad en Internet, 2015:http://www.symantec.com/es/es/security_response/publications/threatreport.jsp

45. Estudio sobre el cibercrimen por la UNODC, oficina de naciones unidas para las drogas y el crimen:

http://issuu.com/spandataartadata/docs/cybercrime_study_210213.

46. CNN- CERT (Centro Criptológico nacional- Gobierno de España): Guías del esquema Nacional de Seguridad: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

47. Sobre Hacking Team aparte de lo explicado en el caso de España, la EFF también se pronunciará al respecto, apuntando a estos como unos delincuentes al servicio de los estados: https://www.eff.org/es/deeplinks/2015/07/raiz-de-la-filtracion-de-hacking-team-eff-y-grupos-de-sociedad-civil-en

48. Assange, J. Cypherpunks. La libertad y el futuro de Internet. Deusto. Madrid. 2014.

4.6 Lucha por la privacidad. Periodismo y hactivismo cívico.

Defender la soberanía individual y la capacidad de ejercer nuestros derechos sobre los datos que generamos en nuestro contacto con la red ha pasado a ser un debate de primer orden en entornos dedicados al Software, la seguridad y la prensa. Que cada vez un número mayor de colectivos y la propia especificidad de cada uno de estos empiece a tratar sobre la privacidad como un elemento prioritario comienza a tener un efecto en la transmisión de contenidos al respecto. Redes sociales, software, aplicaciones, servicios domésticos conectados, cada vez disponen de una mayor cantidad de datos personales sobre los que tan solo se ejerce una limitada capacidad de acceso y modificación. En este aspecto, leyes como las de la protección de datos o la nueva aplicación del reglamento en torno a las *Cookies*, aunque apunten a la recolección de datos no consentida, no han pasado en la práctica de un *banner*, una nota en la cabecera o al pie de las páginas que prestan servicio en España. La realidad de la captación de datos personales es amplia y compleja y afecta a múltiples sectores (1).

Hasta ahora hemos podido describir cómo, estados, empresas y delincuentes convergen en la compulsiva adquisición de datos personales de la mayor parte de los que hacen usos de la red. Curiosamente, la contraparte, es decir la trasparencia en la adquisición y empleo de medios tecnológicos es una de las fuentes más opacas de nuestro tiempo,

provenga de fuentes gubernamentales o empresariales. También al respecto hemos visto como no toda la actividad podía reconocerse abiertamente dado que buena parte de esta podría ser declarada ilegal o afectar a la credibilidad del que la emplee.

En general la censura y el espionaje han sido procesos paralelos en la fase más reciente de Internet. El caso de la vigilancia generalizada de la ciudadanía ha sido especialmente notorio entre las democracias occidentales, que han podido conocer cómo mediante diversos métodos y en nombre de una progresiva fundamentalización del concepto de seguridad, la privacidad que era esperable en las comunicaciones no existía como tal. Como hemos ido viendo a lo largo del trabajo, el momento clave de todo este proceso sería el conocimiento con toda certeza surgido de la cascada de revelaciones que comenzaran con WikiLeaks y terminaran, hasta el momento, con las filtraciones de Edward Snowden (2).

La importancia de la privacidad de nuestras comunicaciones ha llevado, como hemos visto, a bloqueos masivos y diversos intentos de filtrar y conocer el tráfico de red de los ciudadanos. El caso Chino, además del Gran Cortafuegos que limita los servicios extranjeros visibles y utilizables en el país, también existen prohibiciones expresas para el empleo de ciertas herramientas (3). Tal es el caso de TOR, que comenzaría a bloquearse desde 2009, tal y como aseguran desde el propio proyecto, donde afirmaban que prácticamente el 80% de los repetidores públicos eran bloqueados en ese momento por el sistema de filtrado (4).

La extensión de formas de censura y auditoria no solo se circunscribe a estados totalitarios. Hemos visto cómo casos como el británico o el francés, por citar ejemplos muy cercanos, con la excusa de la

contención de usos de archivos con derechos de autor, han dispuesto de formas de auditoria de tráfico que vulneran la privacidad de sus ciudadanos. Así la supuesta defensa de un derecho frente al uso de tecnologías P2P ha hecho que en la práctica existan legislaciones con diversos grados de intensidad en la vigilancia también en Bélgica, Alemania, Italia, Suecia, Finlandia o Dinamarca (5). En general en Europa existen regulaciones activas en lo que respecta a la pornografía infantil y la defensa del copyright. Asimismo, el largo debate sobre la protección de datos y la privacidad vuelve a salir a flote mediante iniciativas recurrentes de diversos estados. Francia, de nuevo con la bandera de la seguridad, acaba de incorporar una "ley de programación Militar" que permite la vigilancia ciudadana sin orden judicial (6)

La comisión sobre derechos civiles de la UE, denominado LIBE, ha planteado debates al respecto a propuesta de grupos de la *eurocámara* en lo que respecta a las directivas como la de protección de datos. A finales de 2015 se tiene previsto una nueva puesta en debate de toda la directiva (7). El reconocimiento de la cantidad de datos que las compañías obtiene voluntariamente e infieren a través de servicios y elaboraciones propias junto el conocimiento de sistemas de recopilación de datos como el llevado a cabo por la NSA, con la necesaria colaboración reconocida de gobiernos como el británico o el alemán, hacen que la posición frente a un eventual cambio favorable a una adquisición y retención de datos por parte de empresas sea visto con gran recelo. Así, se espera un movimiento de contestación a las propuestas que se van conociendo por parte de grupos muy identificados con los intereses empresariales. Campañas como las de *Reclaim Your Data,* en la que convergen varios grupos y organizaciones cívicas, hace especial mención en la forma en la que la actual captación y elaboración de perfiles es capaz de burlar esta legislación europea o queda fuera de su jurisdicción (8).

Empresas, estados, aplicaciones

Todas las fuentes del espionaje terminan por tener como víctima a la ciudadanía. Una de los mayores problemas de la falta de una conciencia del alcance de la disposición de nuestros datos, especialmente significativa en este último periodo de expansión de la conexión a la red. El aumento de la base de usuarios con cuentas en redes sociales, no ha dejado de incrementar la forma en la que estos alimentan la infraestructura del Big Data. Las formas nada claras en las que los apartados dedicados a la restricción de perfiles, la retención de datos o las cláusulas de privacidad, son ubicados en lugares poco usuales en las disposiciones de las páginas y aplicaciones de las redes sociales nos muestran el interés en que siga siendo así (9).

Una de las críticas que intelectuales como Laurence Lessing hace a la sociedad actual es cómo a cambio de la comodidad (la "usabilidad") hemos cedido buena parte de nuestra privacidad. La cuestión más preocupante de ello es que no ha uy consciencia de la importancia del asunto. El tecnocentrismo y la ilusión de la libre elección individual, ha constituido un proceso de sustitución de mitos y de remodelación de la realidad hacia la banalización. El denominado *efecto Disney*, es conocido entre sociólogos como el proceso en el que la imagen sustituye a la realidad y la ciudadanía asume su interacción con el nuevo medio entre lo lúdico y pasivo. Convertir a la ciudadanía en espectadora- consumidora que vea su papel social como un elemento trivial resulta el escenario deseable

para poder hacer uso del instrumental desplegado para la gestión comercial. De nuevo Lessing, acusa a esta sociedad en remodelación como los "Eloi" de H.G. Wells. Un conjunto de individuos sin sentido de responsabilidad, inmersos en la lógica del exceso, la obsolescencia programada y la cultura dirigida (10). En todo ello subyace una concepción doctrinal que trata de asociar la revolución tecnológica como un proceso inherente a una forma única de organización social asociado a la ley del mercado y a la globalización. Quizás por ello y por el propio origen muy ligado a la contracultura (especialmente al movimiento literario del ciberpunk) del mundo del hacking, la contraposición y defensa de modelos informáticos alternativos haya tratado de vincularse interesadamente a movimientos antisistema. Sin duda, la mayor parte de organizaciones de carácter alternativo (en general) suscriben el ideario de defensa de libertades que organizaciones como la *Free Software Foundation*, EDRI o EFF, entre otras defienden. A pesar de ello el peso del análisis tendría que recaer en cómo empresas y legisladores comparte una doctrina no siempre declarada y como ciertos procesos se sustraen al debate en lugar de acusar a organizaciones defensoras de derechos. Esta tensión entre extremos es lo que en nuestros días da origen a legislaciones contrapuestas, no del todo claras y a ambigüedades calculadas. Mientras tanto, condiciones de uso redactadas en lenguaje legal calculadamente arcano y asumibles a golpe de ratón, abre la puerta de la privacidad (11).

La expansión tecnológica no ha ido acompañada de la necesaria educación sobre el uso del medio. La simplificación del empleo ha conseguido por contra que la mayor parte de la ciudadanía tenga hoy en día acceso a la red, aunque no sea consciente de los riesgos y los límites de la cesión de datos que supone. Los términos de uso de la mayor parte de aplicaciones y servicios suelen ser una parrafada que nadie se preocupa el leer. El proceso habitual de *siguiente, siguiente, siguiente*, coloca a los usuarios en una aceptación de servicios que desconocen. La incapacidad

de ejercer un control real, muy a pesar de lo descrito por leyes como la española de protección de datos, deviene en el contexto actual de recolección de datos.

La sospecha del espionaje y la cada vez mayor necesidad de recolectar datos por parte de las empresas no paran de concurrir mecanismos de espionaje o *minería* de datos personales, de los que paulatinamente vamos conociendo sus usos por diversas fuentes. Uno de los más recientes será que de nuevo Lenovo, El gran fabricante chino de portátiles que adquirió la división de esta tecnología de IBM, estaría volviendo a ubicar en sus equipos un software que no se puede eliminar. A principios de 2015 saltaría la primera información a propósito de *Superfish*, un software que la empresa preinstalaba en todos sus portátiles, destinado a recopilar datos de usuario y modificar los certificados instalados en la máquina. Una de las funciones principales encontradas en esta aplicación era la de insertar contenidos publicitarios dirigidos directamente en la navegación. Es decir, que estaban colocando en sus terminales software tipo *Adware* convenientemente oculto en los procesos del sistema para no ser detectado (12).

Sin embargo la compañía, tras este escándalo, no accedería a revelar que mantenía más tipos de software instalados de forma no reconocida. Así, de nuevo en Agosto de 2015, la noticia de la inserción de más *BloatWare* (software Basura) volvería a salpicar a la empresa China, de la mano de usuarios del foro de *Ars Technica* que detectarían la presencia de conexiones no deseadas en sus equipos. Uno de estos, concretamente se conectaba a los servidores de la empresa cuando detectaba una instalación del sistema operativo Windows, en palabras del comunicado de prensa posterior, para “entender cómo usan los clientes nuestros productos" (13).

El caso de Lenovo es tan solo uno de los ejemplos más recientes y visiblemente oscuros de una práctica generalizada. Como ya hablamos cuando tratamos del sistema operativo Android. La inclusión de software de empresas como Google, son la puerta de entrada a su correspondiente ecosistema. Por su parte, vimos como Apple hacía lo propio con su cercado jardín de aplicaciones y servicios. En todos los casos, la permanencia del usuario dentro de su conjunto de productos se convierte en cifras de negocio y alimento para sus diferentes formas de monetarizar el recorrido cotidiano del usuario en la red. Como añadido, muchos fabricantes, han tratado de abrir frentes en los sistemas de Google, Apple o Facebook, insertando dentro de sus dispositivos aplicaciones y servicios propios para tratar de desviar el consumo de sus compradores. Así, empresas como Samsung, son conocidas por la cantidad de *BloatWare* que insertan en el sistema operativo de sus terminales móviles. Aplicaciones no deseadas que como mal menor consumen espacio y recursos, en muchos casos no pueden ser eliminadas sin conocimientos avanzados y que pueden llegar a proceder como software espía (14).

Sin tratar de detallar todos los elementos por los que el software comercial busca sacar partido de sus usuarios, otra de las fuentes clásicas de instalación de productos de seguimiento han sido las plataformas de instalación de software de navegador, las famosas barras y otros productos inoperantes. En este caso, muchos de estos productos se han ganado la valoración como *Adware* (añadidos no deseados) y han caído en la lista de software malicioso de antivirus y software de protección en general. Junto con ello, la profusión de anuncios en plataformas web ha terminado por saturar algunos sitios para convertirlos en lugares poco apetecibles. El modelo de negocio de muchas páginas comerciales y blogs se sustenta en la inclusión publicitaria. Sin embargo, el saber valorar la cantidad asumible por el usuario ha sido una de las fuentes de debate en

el medio. Todo esto nos lleva a la escalada actual de bloqueadores publicitarios. En principio, el empleo de este tipo de herramientas, muy marginal, apenas afectaría a las empresas de publicidad. Sin embargo el aumento de su base de usuarios llevará a situaciones y alianzas extrañas (15). Así AdblockPlus, la aplicación pionera en el bloqueo de publicidad, cambiará la forma en la que gestiona sus *listas negras* y *blancas*, con un nuevo criterio de "publicidad aceptable". En realidad, se pudo saber que la inclusión de ciertas compañías como Google o Amazon en sus listas blancas era parte de un acuerdo comercial. Este movimiento, hará que surjan alternativas a ese bloqueo con origen libre. En móviles Android, *Adaway*, de la que ya hemos tratado, será una de los Aplicaciones más extendidas, hasta el extremo que Google la retiraría de su tienda de aplicaciones y hoy en día hay que acudir a su web o a tiendas alternativas como *FDroid* para su descarga. En los navegadores convencionales, alternativas como *Ublock* serán mucho más eficaces y permitirán poder extraer temporalmente partes de la web bloqueada si así lo necesitamos. El crecimiento de este tipo de bloqueos ha comenzado a preocupar al entorno comercial. Pagefair, uno de los líderes de la inserción publicitaria, señalaría en su informe sobre el avance del bloqueo publicitario para 2015. En este, se apunta a que existen cerca de 200 millones de usuarios de diversos sistemas de bloque publicitario en el mundo. Una cifra que no ha parado de crecer como consecuencia de la expansión y el abuso del empleo de añadidos en las páginas webs. Las cifras de crecimiento llegarían al 82% en el mes de junio de 2015, algo que preocupa a estas empresas que se autodefinen como defensoras de la web de acceso gratuito (16).

Al respecto de los elementos de seguimiento de navegación, que ya no solo lo componen las cookies sino que se han desarrollado mecanismos mucho más avanzados, no todos ellos hechos públicos. Organizaciones como EFF han desarrollado aplicaciones propias para como Privacy Badger, un añadido al navegador que se emplee (con versiones para los

más extendidos) que impide y bloquea el seguimiento, alertando asimismo de qué tipo de rastreo y que destino tiene en cada caso (17).Desde 2011, herramientas de búsqueda y bloqueo como *Disconnect*, o *AnonymoX* han prosperado entre un público menos especializado pero saturado por la publicidad. En muchos casos, el exceso de los medios ha sido el detonante para que la toma de consciencia sobre la realidad del entorno de internet se abra paso (18) (19). De nuevo será la tecnología asociada a los dispositivos móviles la que más avance al respecto. Los modelos de aplicaciones *Fremium,* gratuitas con publicidad y con compras integradas para poder mejorar la experiencia de uso, se han extendido en los mercados de cada ecosistema (20).

Entre los casos más curiosos en lo que respecta a la interpretación de las libertades del usuario, destacaríamos el de Google que por un lado colaborarían con el espionaje de la NSA pero luego se muestran inflexibles contra estados como China. Eric Smidt, presidente de Google, acusa a China de ser la potencia que mayor grado de espionaje industrial mantiene, con cifras alrededor del 80%. Para ello no duda en ofrecer la alternativa de un tráfico de Internet completamente cifrado como solución a la privacidad (21). La reacción por parte de Google se explica por su abandono del país al no poder atender las peticiones de acceso que el gobierno Chino pretendía a su buscador y sus servicios. Finalmente China, elevaría el llamado *Gran Firewall Chino*, un servicio de restricción de contenidos externos que mantiene parte del Internet chino al margen del resto del mundo, y potenciaría *Baidu* como el gran servicio sustituto de los que hasta entonces ofrecía la gran G (22).

Google Now, Cortana, Siri o el reciente *Facebook M*, son nombres de sistemas de asistencia al usuario por medio de interfaces sencillas, creados respectivamente por grandes de la red como Google, Microsoft, Apple y Facebook. Todos ellos parten de la base que para reconocer las

pautas del usuario deben ser capaces de alimentar primero un Big Data con capacidad como para saber reaccionar a ubicaciones, momentos concretos y búsquedas. Esto significa, que la recolección de datos de carácter personal que el usuario debe ceder a estos sistemas, integrados en bases de datos ubicadas en la radicación de cada centro de datos de estas empresas, debe ser muy grande. Con ello, a cambio de la comodidad de tener respuestas que buscamos y que incluso la máquina llegue a adelantarse a nuestros deseos de consulta en la red, hemos nutrido una base de datos que recolecta buena parte den nuestro discurrir no solo en la propia red sino nuestras posiciones, mediante usos de tecnologías de posicionamiento como la del GPS, y nuestro entorno, por ejemplo con las interacciones con otros usuarios, amigos, compañeros de trabajo y el etiquetado y ubicación de nuestras fotografías. Así, vemos como de forma voluntaria y casi inconsciente se alimenta una maquinaria frente a la que no tenemos derecho de retracto. Incluso si no hemos cedido nuestros datos, las bases de datos en función a quien lo haga en nuestro entorno pueden ser capaces de elaborar un perfil personal bastante preciso. El fin de todos estos servicios, ofrecidos de forma gratuita, persigue una clara función comercial. Nuestros datos personales son parte del negocio mediante el que nos ofrecen productos que encajen en nuestro perfil, privilegien ciertos servicios, que les conviene y nos sugieran ciertas pautas en beneficio propio. Así, automatizar buena parte de nuestras vidas ha convertido a las máquinas de Google, Microsoft, Apple o Facebook, en auténticos orquestadores de la vida privada de cada vez más usuarios, de forma desatendida e imperceptible. De nuevo la comodidad frente a la privacidad abre una brecha en la que el entorno comercial gana (23).

Como último apunte, hemos visto como las empresas con sede en EEUU ceden en mayor o menor medida datos de sus usuarios a peticiones judiciales o policiales en función a las diversas legislaciones de retención de datos que se han ido sucediendo en dicho país. El debate surgía cuando se entendía que las redes sociales y grandes aplicaciones y servicios de la

red se encontraban radicadas en dicha nación. Por tanto, era un hecho que los datos de sus usuarios, sin importar la procedencia, se encontraban finalmente expuestos al cuerpo legislativo estadounidense. A esto se unía la presión que agencias como la NSA había llevado a cabo y la colaboración, más o menos voluntaria que estas compañías ofrecían. EL informe de la EFF sobre el comportamiento de las principales empresas de la red es esclarecedor del grado de cesión de datos que finalmente estas ofrecen al este gobierno y sus organizaciones (24). La escasa confianza que la mayor parte de estas compañías, sobre todo tras confirmarse la existencia de "puertas traseras" dentro de sus plataformas para el acceso a datos, incluso cifrados, inspiran a los redactores del informe está debidamente justificada. Como vimos en su momento la reacción pública de buena parte de estas se consolidaría en una propuesta de regulación estatal, suficientemente difusa como para que se interpretara entre miembros del medio tecnológico como una operación de maquillaje publicitario. La certeza de que Google, Facebook, YouTube, Microsoft, Yahoo!!, Skype, AOL y Apple han colaborado con el programa de espionaje de la NSA denominado PRISM adquiere un peso especial ante la mencionada intención de modificar la directiva europea de protección de datos y las consecuencias sobre el resto de legislaciones de los países miembros (25). En este caso la exposición de datos ciudadanos podría verse incrementada, sobre todo si se plantean los tribunales arbitrales que también están negociándose en el TPP (del que ya tratamos en el capítulo 3.2). En este contexto vemos cómo se vuelve a producir una carrera entre la imposición de intereses lobistas y las libertades y derechos civiles, en los que la clave vuelve a ser la capacidad de filtración de negociaciones a puerta cerrada. Mientras Campañas ciudadanas *como Naked Citizens (*26) o *Reclaim Your Data* (27), quieren fortalecer la legislación de protección de datos y descartar la posibilidad de ampliación de capacidades de retención y tratamiento de estos por parte de las empresas, la aceleración de estas negociaciones apunta a un interés por consolidar posiciones contrarias. Tal carrera ha llegado a extremos de

que la plataforma de filtraciones WikiLeaks ha llegado a ofrecer 100.000 dólares a quien les suministre documentación sobre estas negociaciones opacas (28). Hasta el momento, se conocen ciertas correspondencia ya filtrada en la que se apunta que las legislaciones estatales debe plegarse al interés empresarial transnacional en cuanto a sectores estratégicos y servicios públicos, basándose en "el interés comercial" (29).

En España, una de las últimas cuestiones de la que se ha suministrado escasa información es la elaboración de un proyecto denominado *PNR, Sistema de Registro de Nombres de Pasajeros (*Passenger *Name Record)*. En la UE, La LIBE (Comisión de Libertades Civiles, Justicia y Asuntos de Interior) rechazaría una propuesta similar de ámbito europeo, paralizando el posterior debate al respecto (30). Sin embargo, el gobierno español, decidiría mantener la idea y desarrollarla en el entorno de sus fronteras. La supuesta idea de establecer un control de viajeros en las fronteras del estado oculta la elaboración de una serie de perfiles personales, elaborados a lo largo de las publicaciones en redes sociales, que significaría la posesión de un fichero con perfiles ideológicos por ejemplo . La agencia de protección de datos recoge la idea en un comunicado en el que cita a las autoridades europeas de protección de datos, cuando afirmaban que la elaboración de ficheros previstos en el PNR puede "debilitar seriamente los derechos a la protección de la vida privada y de los datos personales de todos los viajeros, derechos estos reconocidos por los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea" (31). Sin embargo, el ministerio de interior llevaría adelante el proceso de publicación del pliego y el presupuesto, valorado en 1,6 millones de euros y la adjudicación, en agosto de 2015, para un sistema que se pretende tener funcionando, según informa el propio pliego, antes de finalizar el año (32).

Hackers, periodistas y activismo por los derechos y libertades

La brecha actual entre los derechos individuales expresados por los enunciados democráticos que definen a la mayor parte de los estados de corte occidental y la realidad en la que la red se está conformando supone la concreción más evidente del periodo de relativización y disolución de los principios democráticos que fundamentaron a estas democracias. La cantidad de situaciones en las que el ejercicio de derechos básicos o el propio periodismo de investigación o comprometido puede exponer a quien lo lleve a cabo crece con la propia extensión de la red (33). Como hemos señalado a través de todo nuestro trabajo, en esta constante pugna de intereses en la red la principal perjudicada ha sido siempre la ciudadanía que ha visto como empresas, estados y delincuentes, pugnan por acceder de un modo u otro a sus datos personales y disponer de ellos con una impunidad de diversos alcances. La opción que le queda, al margen de permanecer como un usuario-consumidor al arbitrio de tales circunstancias, es la de tomar opción activa por la defensa de sus derechos y hacer uso de las herramientas que se pueden emplear para el caso (34). El cifrado, el control de la privacidad y el rechazo a una cultura dirigida y al fundamentalismo de la seguridad que se ha terminado de imponer a lo largo del presente siglo, son parte de esa actitud. Resulta complejo, una vez desplegados todos los elementos que componen esta realidad de la red de nuestros días, no tener conformada una opinión y apuntada la opción. Tampoco existen muchas alternativas más allá de la pasividad y la complacencia, que son la postura generalizada. La cultura del activismo cívico, juega en este escenario un papel central como único elemento capaz de ofrecer una alternativa al tejido de una realidad que quiere

ofrecerse como única opción posible. El siguiente paso para reivindicar el papel de soberanía ciudadana es el de la autodefensa en Internet (35).

La libertad de prensa es uno del os frentes en los que la maduración de las formas de empleo de las herramientas seguras de comunicación en la red más avanza (36). La persistencia del control y la censura en diversos países, junto con el conocimiento actual de las más evolucionadas formas de auditoría por parte de servicios de espionaje vinculados de un modo u otro a los gobiernos, han impulsado un proceso en los medios periodísticos más comprometidos en el que el cifrado y la ocultación de usos de la red comienzan a ser prácticas habituales de una nueva gestión del sentido común en las redes (37). La especial situación de la prensa en este sentido ha favorecido la labor la extensión de los métodos de salvaguarda y contraespionaje. La implicación de nuevos agentes en el frente contra la vigilancia ha posibilitado una ampliación en el rango de alcance y credibilidad de todas las cuestiones relativas a la defensa de la privacidad (38).

La ventaja del conocimiento de los últimos tiempos ha sido la de saber con certeza los métodos y limitaciones que los diversos sistemas de auditoria y recolección de datos personales tienen. Así, por parte de la propia NSA hemos podido saber que cifrados para las comunicaciones como el PGP son una de las piezas más complejas de intervenir (39). Por ello, el papel central del cifrado en todo este proceso es fundamental. Como veremos, también por ello, es uno de los frentes legislativos en los que diversas autoridades quieren intervenir. Junto con ello, el establecimiento de canales seguiros de comunicación, la evasión de formas de intervención de las comunicaciones, el uso de redes privadas virtuales, conocidas como VPN para canalizar los datos y el cambio de las DNS, los servidores que interpretan nuestras peticiones de acceso a la red,

hacia servidores que garanticen la privacidad son pasos esenciales en el "bastionado" de nuestro acceso (40).

Como hemos podido ver buena parte de las campañas que diversos grupos de activistas de los estados democráticos de corte occidental han mantenido han hecho especial mención al derecho a la privacidad. En lugares donde no se aplican los derechos fundamentales esto tiene especial importancia dado que la capacidad de mantener sistemas privados de comunicarse puede marcar la diferencia respecto a la persecución (41). Aun así, las fuentes coinciden en que la importancia de la defensa de estos derechos radica en la imposibilidad de ejercer otros derechos básicos si cuestiones tan radicalmente sustanciales de cualquier democracia son cuestionadas bajo cualquier pretexto. Hasta el momento, debería ser la investigación judicial, con su permiso correspondiente, la única forma de permitir una intervención en la intimidad de las personas, como bien apuntan fuentes como el propio Juez Eloy Velasco. La divisoria entre los derechos cívicos y la investigación debería quedar justificadamente circunscrita (42). En otros casos, todas las fuentes del activismo cívico apuntan a que la protección del derecho debería primar sobre cualquier interés empresarial (43).

Otra de las fuentes de lucha de las organizaciones ha sido el de la defensa de la neutralidad de la red y el derecho a que el software no pueda ser restringido, como se pretendía con las patentes de software.

También hemos podido ver como la disonancia entre los usos y formas de una ciudadanía habituada a una cultura de acceso y las viejas formas orientadas a restringir los derechos de autoría y tratar de sacar rentas constantes de ello, incluso forzando la forma en la que la red existe, ha constituido otra de las constantes. El DRM, ha significado el último

intento de restringir las maneras en las que se puede disfrutar de contenido digitales. Su fracaso, es la evidencia de cómo una correcta defensa de los derechos de los creadores no tiene por qué entrar en conflicto con sus usuarios ni pasar por una criminalización preventiva global de sus usos. El poder plegarse a las necesidades que ya expresan y se organizan por medios alternativos es una posición más inteligente que nuevos medios como los que se dedican al *streaming* musical y posteriormente al consumo audiovisual han abierto (44).

Como ya hemos visto a lo largo de nuestro trabajo, la fuerte construcción y elevación de legislaciones que recurrentemente tratan de poner el ejercicio de patentes y derechos de autor como parte privilegiada del empuje de los gobiernos son una de las formas más evidentes de rastrear el poder de la empresa sobre los estados. El ejemplo recurrente de *Mickey Mouse*, que nos explica Laurence Leesing para detallar cómo la legislación sobre el copyright americano (la DMA) se ha modificado cada vez que los derechos de autor del conocido personaje de animación se aproximaba al dominio público, es uno de los que con más claridad no explica la manera y los ritmos a los que obedece el marco legislativo de naciones como EEUU, que cada vez se hace más extendido al resto de estados (44).

La contrapartida de todo este proceso es que la realidad del hactivismo, como hemos venido a definir al activismo más orientado al empleo de tecnologías para la consecución de sus objetivos, todavía se encuentra en proceso de formación de estructuras formales. Su situación es la clásica en todos los procesos sociales de nuestro tiempo, la fragmentación. La gran ventaja de este activismo adaptado al empleo de internet es su capacidad de difusión por el nuevo medio y el conocimiento de los instrumentos para desmontar procesos ocultos (46). La maduración de estos movimientos a lo largo de la segunda década del siglo, ha venido

acompañada de un conocimiento más profundo de la capacidad de estados y empresas de modificar contextos sociales. La denuncia y la revelación son por ello dos de los instrumentos principales de este tipo de organizaciones enfocadas en una posición defensiva ante el empuje de quienes controlan el negocio en la red (47).

La guerra del cifrado

Como hemos visto, en el cifrado está la clave futura de una red capaz de garantizar las libertades ciudadanas. A lo largo de todo nuestro trabajo hemos apuntado los elementos de riesgo a las libertades, las formas de control y el empleo de los datos de la ciudadanía. Conocido todo esto, el hactivismo comprometido tiene en el cifrado la esperanza de que puede ser el instrumento decisivo en toda esta pugna. Hasta tal punto el cifrado de datos ha tomado una posición central en esta guerra de posiciones en la red que muchas de sus fuentes son en nuestro días el nuevo escenario de confrontación (48).

Como afirma Amy Goodman, de la ONG Democracy Now, criticando el informe "*Going Dark: Criptografía, tecnología y el equilibrio entre seguridad pública y privacidad*" un documento debatido en comisión del senado estadounidense en donde, sumariamente, se exigía la eventualidad de permitir una puerta trasera para burlar la seguridad del cifrado de las tecnologías más recientes, el mantenimiento de la privacidad de las comunicaciones es esencial en cualquier democracia. Miembros de las diversas agencias de inteligencia y del FBI estadounidense, pretenden que se legisle al respecto para mantener esa vía abierta de forma obligatoria para empresas de dicho país (49). Efectivamente, el gobierno estadounidense y británico, ya se han planteado poder legislar al respecto, dado que hasta ahora el juego se había desarrollado mediante medidas de

presión y o mediante un asalto a las formas precedentes de comunicación. Por otra parte, en las actuaciones contra las filtraciones periodísticas de Snowden, realizadas a través del diario británico The Guardian, se confirmaría accidentalmente una documentación secreta del GCHQ acerca de cómo proceder con los dispositivos que contengan información considerada peligrosa. Efectivamente, en Julio de 2013, agentes de la inteligencia británica irrumpieron en la redacción del periódico y procedieron a la destrucción de los dispositivos del periodista Glen Greenwald, alegando un supuesto código de seguridad nacional desconocido (50). Los agentes emplearon un protocolo bien determinado que incorporaba herramientas tan sofisticadas como un "degausser", que es un dispositivo que provoca el borrado de dispositivos magnéticos. Este hecho corroboraba la filtración de WikiLeaks sobre documentos de 2001 del ministerio de defensa británico que obligaba a la destrucción de información para protegerse de "grupos extremistas, periodistas de investigación y terroristas" (51).

Diversos casos nos han mostrado la importancia que el cifrado de datos tiene en la red. Uno de los ejemplos que más revuelo causara en el medio sería el del cierre brusco de la empresa Lavabit. La compañía, contaba con un producto estrella, un servicio de correo cifrado y seguro. Precisamente sería E. Snowden quien lo popularizaría al comentar que era el servicio de correo que empleaba habitualmente ya que mantenía una forma segura de comunicación cifrada. La presión del gobierno estadounidense, que irrumpiría en la empresa y obligaría a sus creadores primero a insertar dispositivos de control de tráfico y luego que les revelaran las claves privadas para acceder a todos los datos de usuarios terminaría por hace que estos optaran por cerrar un servicio que surgiera en 2004 como alternativa al correo de Google, Gmail, que escanea los contenidos de los correos de sus usuarios. Esta decisión haría que Ladar Levison, el

propietario, tenga que enfrentarse a un proceso judicial por no responder como se le solicitaba a la llamada "carta de seguridad nacional" (52).

Bruce Schneier, otra de las voces más señaladas en lo que respecta al cifrado y la defensa de la privacidad en las comunicaciones explica en su libro "Data y Goliat: Las batallas ocultas para recopilar tus datos y controlar tu mundo", como la progresión hacia la intervención de todos los medios tecnológicos puede hacer que muchas de las empresas realmente preocupadas por la seguridad emigren de EEUU, ante la presión del gobierno y sus agencias (53). Tal ha sido el caso de Phil Zimmermann, creador del cifrado PGP (Pretty Good Privacy), del que ya hemos tratado, que decidiría a primeros de 2015 abandonar EEUU y ubicar su empresa en Suiza, donde las leyes sobre la privacidad son más protectoras (54). La compañía Silenc Circle, fundada por este en 2012, se dedica especialmente a las conexiones seguras y tiene como productos estrella un dispositivo telefónico, denominado *Blackphone* , con un derivado de Android y aplicaciones de comunicación cifradas y seguras, como *Silent text,* que son de las aplicaciones más confiables según contrastara la EFF (55).

De todos los casos de herramientas polémicas respecto a la seguridad y el cifrado, *TrueCrypt* ha sido la más destacada. De creadores desconocidos, la aplicación capaz de funcionar en buena parte de los sistemas operativos, era capaz de cifrar discos duros enteros, crear unidades ocultas o cifrar datos concretos. Todo ello con una interfaz sencilla de emplear que la había convertido en la aplicación favorita de buena parte de los usuarios más comprometidos. El repentino cierre de la aplicación y las extrañas aseveraciones de su equipo de desarrolladores, que recomendaban el empleo de la herramienta de cifrado *Bitlocker* de Microsoft, algo muy llamativo, pondrían sobre aviso a usuarios sobre la inconveniencia de instalarse la versión 7.2. (56) Mientras tanto, la

herramienta estaba siendo sujeta a un proceso de auditoría de seguridad para comprobar la robustez del sistema de cifrado. En el entorno hacker, esto sugería de inmediato un *warrant canary,* una forma de revelar sutilmente que la herramienta está siendo investigada (57). Esta será una de las interpretaciones más difundidas en foros dedicados a la seguridad. Las pistas sobre que pudiera estar siendo investigado por agentes del gobierno suele darse mediante errores en las publicaciones, como fechas de actualización anunciadas que no se cumplen, o como en este caso citar a BitLocker, expresamente rechazado por los desarrolladores con anterioridad, lo que conforma por sí mismo una pista clara de tales hechos. La herramienta en cuestión estaba teniendo, como hemos dicho, una auditoria de seguridad (58). El proyecto Open Crypto Audit Project, financiado con una campaña en internet, publicará sus conclusiones en abril de 2015. En estas aunque se encontrarían ciertos errores en el software para Windows, que podría debilitar la fortaleza del cifrado, según el que se elija, pero no se encontró puertas traseras ni cadenas de código sospechoso (59). Con ello, buena parte de la comunidad de usuarios de la herramienta pudo seguir empleando la versión 7.1 con cierta confianza, abandonando completamente la versión 7.2, publicada junto con la advertencia antes descrita. Pronto aparecería una página con datos del proyecto y dos grupos de investigación para ofrecer desarrollos derivados de la herramienta principal.

Asociaciones como *Pure Privacy,* localizadas en suiza, tratan de establecer una serie de aplicaciones similares con garantías de privacidad. Para ello, testean y mantienen relaciones con desarrolladores de código abierto en la búsqueda de una lista de proyectos debidamente auditados para ser acreditadas como protectoras de la privacidad. Su foco principal es la sustitución de la *TrueCrypt* por una herramienta más sofisticada y segura. Actualmente hay dos proyectos derivados de este para ofrecer una sustitución conveniente: *VeraCrypt* y *CipherShed* (60).

El cifrado y la posesión de nuestra privacidad de ha convertido en los últimos tiempos en todo un signo de higiene democrática. Dado que la confianza que pueda tenerse en las formas más transparentes de navegación y comunicación en la red no existe, ante la quiebra creada desde la puesta en conocimiento de los métodos de espionaje cada vez más extendidos y a la inseguridad creciente en torno a las comunicaciones en la red, el cifrado y la ocultación de rastro van camino a convertirse en una práctica generalizada. EL informe de la Comisión de Derecho Humanos de las Naciones Unidas, redactado en mayo de 2015, confirma que el derecho al cifrado debe ser considerado como parte del derecho a la intimidad y la libre expresión (61). Con ello, se apunta en sentido contrario a las intenciones legislativas arriba descritas y sitúa el debate de nuevo en la confrontación de derechos. Tratando de mediar entre ambas posiciones, la ONG Acess Now, que muchos identifican con el interés de la gran empresa norteamericana que defiende libertades ajenas, ha preparado un primer encuentro llamado *Crypto Summit 2015,* para iniciar un debate sobre el empleo del cifrado (62). Sin embargo, conocer a los patrocinadores del evento nos coloca adelante la visión que tendrán sus eventos.

Mientras todo este proceso continúa, las filtraciones se han convertido en la fuente principal de información acerca de cómo actúa la parte más oculta de los gobiernos. Así el diario alemán *Der Spiegel*, podría hacerse en diciembre del 2014 con un conjunto de documentos sobre la NSA que publicaría en un reportaje sobre la clasificación interna de los niveles de dificultad de diversos servicios y aplicaciones. Por ejemplo, PGP todavía sigue sin ser descifrable. Los analistas de la NSA todavía no han podido romperlo y por tanto des uno de los métodos más seguros de envió de texto (63). En los documentos, existen guías de criptoanálisis, de comunicaciones de Voz por IP o de cómo intervenir

comunicaciones de Skype. El nivel de detalle del informe lo convierte en una de las fuentes más documentadas que se tienen respecto a los métodos de espionaje de la NSA y su nivel real de conocimientos. Por poner algunos ejemplos de los datos encontrados, los analistas de la agencia catalogan como "trivial" el rastreo de un documento en la red o la intervención de comunicaciones del chat de Facebook. Acceder a una cuenta del servicio de correos electrónicos ruso *mail.ru* se cataloga como de dificultad moderada. Sin embargo, el cifrado de TOR, todavía les causa dificultades, así como la mensajería de "Off-The- Record" o las llamadas mediante Repone. TrueCrypt también aparece como una de las amenazas a su capacidad de intrusión (64). Otras vías de las que ya tratamos como el uso de VPN o HTTPS, no garantizan la seguridad respecto al espionaje. Junto a esto, el manteamiento de contraseñas por defecto en la mayor parte de infraestructuras y hardware con conexión a la red, abren una puerta a su posible intervención. Junto con todo el despliegue tecnológico y la recopilación de conocimientos también ciertas prácticas cotidianas podrían mantener mayores niveles de privacidad. El proceso de maduración y la capacidad de una educación en la seguridad de nuestros medios podría residir una de las claves en la vuelta a un estado de la cuestión en el que no se viva en un atropello contante.

La puesta en conocimiento de todas estas cuestiones ha comenzado a movilizar a la ciudadanía en pos de su seguridad. Uno de los más recientes movientes ha sido el de la inutilización del chip de identificación de los nuevos documentos de identidad alemanes. Uno de los documentos de la NSA, hacía mención a la capacidad de una lectura de un rango más amplio que el declarado (65). Esto significaría una capacidad de control del que no han sido advertidos los ciudadanos alemanes. Mientras muchos optaran por el sistema de la *Jaula de Faraday* (aislando el chipo dentro de un cuerpo metálico), otros procederían a potenciar una campaña para quemar estos Chips introduciendo los carnet en el horno microondas. De hecho una de las más recientes informaciones

que se tienen respecto a uno de los sistemas de recopilación de datos personales de la NSA, llamado XKeyscore, confirma que la BFV (agencia de inteligencia alemana) intercambiaba datos de sus ciudadanos a cambio de acceso a datos de dicho programa (66).

Las formas de espionaje y las nuevas técnicas de evasión han evolucionado en los últimos tiempos, mientras la red crecía y se extendía a lo largo de cada vez más elementos de la vida cotidiana. Como hemos visto, diversas organizaciones han elevado la voz de alarma sobre el proceder de redes sociales y empresas que prestan servicios de Internet (67). De forma paralela, sobre todo gracias a grupos de creadores comprometidos con el software libre, se han creado nuevas herramientas comprometidas con la privacidad, con un éxito desigual pero que cada vez se conforman más como alternativas. La dicotomía descrita entre de la comodidad o la privacidad es una cuestión que afecta al conjunto de una humanidad cada vez más conectada (68).

Una sociedad incapaz de elevar el ejercicio de sus derechos permite con su inacción el avance de las medidas de quienes diseñan su estrategia conociendo perfectamente este hecho. El conflicto permanente entre una legislación con una tendencia hacia la desproporción vigilante y sancionadora y la defensa de las libertades cívicas es la fuente principal de todo este proceso.

Mantener a la ciudadanía en un estado de vigilancia permanente por la eventualidad de un comportamiento terrorista no es solo un atropello a las libertades sino una auténtica declaración de intenciones de quien tan solo lo sugiera. Las fuentes de los problemas de la sociedad actual no se resuelven mediante el espionaje ciudadano. El estado de madurez por venir

puede significar retomar la soberanía individual y colectiva sobre nuestras vidas o una cesión al modelado social

---

NOTAS

1. El portal de la Agencia Española de Protección de Datos contiene toda la información detallada sobre la legislación en torno a las cookies:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/cookies/index-ides-idphp.php , también se creó un portal al detalle para implantarla en: http://politicadecookies.com/index.php

2. VV.AA. Sociedad Mediatizada. Gedisa. Barcelona.2007

3. La información de TOR Project acerca de los primeros bloqueos chinos pude ser consultada en su blog:

https://blog.torproject.org/blog/tor-partially-blocked-china

4. Informe de la UNESCO sobre la censura de internet. Freedom of Connection, Freedom of Expression, disponible en: http

5. Mapas e informes de Open Net Iniciative sobre la censura y los medios de vigilancia en Internet. En este apartado destacaremos el informe dedicado a Europa, donde se hacen mención a los mecanismos de vigilancia ilegales tanto por estados como por empresas. http://map.opennet.net/filtering-pol.html

https://opennet.net/research/regions/europe

6. *La cuadrature du net;* junto con Statewacht, son dos 23de las organizaciones que hace un seguimiento más estrecho a las legislaciones de la UE. En este caso en lo relativo a la privacidad

podemos ver todos
sus informes en: http://www.laquadrature.net/en/Privacy . En cuanto a la nueva legislación francesa, más información sobre el estado actual en: http://www.laquadrature.net/en/huge-threats-to-fundamental-freedoms-and-rights-consolidated-in-the-french-parliament

7. La directiva de protección de datos que data de 1995, disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML se encuentra en debate y se espera que la modificación sustancial de ciertos contenidos favorecerá los intereses de las empresas

8. Reclaim Your Data es una campaña de diversos grupos y organizaciones para que la ciudadanía siga manteniendo la capacidad de controlar los datos personales: http://www.reclaimyourdata.eu/

9. Echeverría, J. Los señores del aire. Telépolis y tercer entorno. Destino. Barcelona. 1998

10. Lessig.L. Por una Cultura libre. Cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad. LOM. Santiago, 2005. Edición electronica: http://www.traficantes.net/libros/por-una-cultura-libre

11. VVAA. Internet y Lucha política: Los movimientos sociales en la red. Capital Intelectual, Buenos Aires, 2006

12. El comunicado de Lenovo al respecto tampoco clarificaba debidamente, la necesidad de las funciones que parecía argüir para justificar su inclusión no declarada. En teoría argumentan que Superfish, un software de una empresa radicada en Palo Alto (California) "mejoraría la experiencia en las compras del usuario": http://news.lenovo.com/article_display.cfm?article_id=1929

13. Los foros de usuarios de *Ars Technica* volverían a revelar los extraños procesos iniciados en los ordenadores de la firma. Esta vez desde la propia BIOS UEFI, que accedía a los servidores de

la empresa para proceder a la instalación de software de las empresas con objetivos no declarados ni consentimiento previo del usuario.

http://arstechnica.com/civis/viewtopic.php?p=29497693&sid=ddf3e32512932172454de515091db014#p29497693

14. Gillmor, D. Nosotros el medio. 2004. Libro disponible con licencia Creative Commons en: http://www.hypergene.net/wemedia/espanol.php

15. AdblockPlus, se defendería estableciendo unos criterios de publicidad aceptable: https://adblockplus.org/es/acceptable-ads

16... Page Fair, empresa vinculada a la publicidad en la red., ha elaborado un informe sobre el crecimiento del bloqueo publicitario de los usuarios de internet hasta 2015, titulado " The 2015 Ad Blockig Report" disponible en: http://blog.pagefair.com/2015/ad-blocking-report/

17. Privacy Badger, es uno de los gestores de privacidad en las conexiones web más famoso, creado por la EFF: https://www.eff.org/privacybadger

18. Disconnect, un bloqueador y buscador alternativo que garantiza la privacidad: https://disconnect.me/

19. AnonymoX, ofrece incluso el cambio de IPs de sus usuarios para dificultar su rastreo: http://www.anonymox.net/en

20. VVAA. The Practice and Policy of Global Internet Filtering. MA: MIT Press Cambridge, 2008. Recurso disponible en: http://www.opennet.net/accessdenied/

21. Como ya señalamos en el capítulo correspondiente a la ciberguerra, la llamativa posición del CEO de Google respecto a los ataques chinos, debemos verla en perspectiva en primer lugar por la propia salida de Google y sus servicios de China y del papel competidor que juegan plataformas locales como Baidu desde entonces, así como el desarrollo

de aplicaciones similares a las que desarrolla la propia compañía. Todo ello, en su última publicación: http://www.newdigitalage.com/

22. Assange, J. cuando Google encontró a WikiLeaks. LMD-Clave Intelectual. Madrid. 2014

23. Lessig.L. El código 2.0. Traficantes de sueños (licencia Creative Commons), Madrid. 2009.

24. El informe de la EFF, llamado "W*ho Has Your Back? 2015: Protecting Your Data From Government Requests* report" detalla las posiciones de las empresas estadunidenses y su práctica respecto a la cesión de datos de sus ususarios: https://www.eff.org/who-has-your-back-government-data-requests-2015

25. La web PRISM Break, suministra herramientas para poder escampar de la vigilancia de sistemas como PRISM: https://prism-break.org/en/

26. La campaña *Naked Citizens (ciudadanos desnudos)*, Llevada adelante por buena parte de las asociaciones de derecho europeas apuntan a la necesidad de retomar el control de nuestros datos. https://www.nakedcitizens.eu/

27. *Reclaim Your Data* es una campaña de diversos grupos y organizaciones para que la ciudadanía siga manteniendo la capacidad de controlar los datos personales: http://www.reclaimyourdata.eu/

28. En el portal de WikiLeaks podemos ver la campaña que han lanzado para adquirir información sobre el TPP antes de que comiencen los acuerdos: https://wikileaks.org/pledge/#rd-6 https://wikileaks.org/WikiLeaks-goes-after-hyper-secret.html

29 Algunas filtraciones ya publicadas por WikiLeaks apuntan a la intencionalidad no manifiesta del TPP: https://wikileaks.org/tpp-soe-minister/

30. La LIBE, Comisión de Libertades Civiles, Justicia y Asuntos de Interior, rechazaría en 2013 la propuesta de control de pasajeros., quedando

desde entonces paralizado el debate: http://www.europarl.europa.eu/committees/en/libe/reports.html

31. La Agencia española de protección de datos tan solo emitirá un comunicado de prensa al respecto: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_02_06-ides-idphp.php

32. En el pliego de condiciones, publicado en febrero de 2015 para el que se puede consultar a través de la cache de google, se hace mención a un importe de 1,6 millones de euros para la elaboración del proyecto:

http://webcache.googleusercontent.com/search?q=cache:pwtE8zJhlYUJ:https://contrataciondelestado.es/wps/wcm/connect/d5ac30f5-4ed4-4bba-8f9b-055a247de6b0/DOC_PIN2015-016021.pdf%3FMOD%3DAJPERES+&cd=5&hl=es&ct=clnk&gl=de

33. Informe de Reporteros Sin Fronteras. "Enemigos de Internet 2014: organismos en el epicentro de la censura y la vigilancia": http://www.rsf-es.org/news/rsf-publica-el-informe-enemigos-de-internet-2014/

34. Informe de Reporteros Sin Fronteras. "Enemigos de Internet 2014: organismos en el epicentro de la censura y la vigilancia": http://www.rsf-es.org/news/rsf-publica-el-informe-enemigos-de-internet-2014/

35. *Privacy Internacional* y *Amnistía internacional* han publicado un informe sobre el estado de la cuestión de las revelaciones de Edward Snowden titulado "*Two Years after Snowden. Protecting Human Rights in an age of mass surveillance"*. Disponible en: https://www.privacyinternational.org/?q=node/591

36. Periano, M. El pequeño libro rojo del activista en la red. eldiario.es libros. Madrid. 2015

37. LA IPI (International Press Institute) ha elaborado un documento sobre el cifrado y el anonimato en la red, titulado "Special report: Encryption, anonymity as safeguards for press freedom" explicado en:

https://www.ifex.org/international/2015/08/21/encryption_anonymity/?i=1 y disponible en http://ontheline.freemedia.at/special-report-encryption-and-anonymity/

38. Actualmente se han diseñado multitud de guías sobre la protección de datos, formas de anonimato en la red pero las más destacadas son: https://info.securityinabox.org/es y la guía de autodefensa contra la vigilancia de la EFF: https://ssd.eff.org/es . Al final del presente capítulo sintetizamos algunas de las más destacadas para empezar a orientarse en una red segura.

39. Para conocer el cifrado PGP y cómo emplearlo, existen múltiples guías en la red como la suministrada por la campaña de autodefensa del correo electrónico, llevada adelante por la FSF: https://emailselfdefense.fsf.org/en/

40. Barandiaran, X. Activismo digital y telemático. Poder y contrapoder en el ciberespacio. 2003. Recurso disponible en http://www.sindominio.net/~xabier/textos/adt/adt.html

41. Himanen, P. La ética del hacker y el espíritu de la era de la información. Destino. Barcelona. 2004

42. El Juez Eloy Velasco, haría una intervención magistral en la II Curso de Peritos telemáticos Forenses, celebrada en Madrid en septiembre de 2014, defendiendo el equilibrio entre los derechos personales y la necesidad de investigación criminal. Al respecto, afirmaba que una intervención superior a un mes debía de ser suficientemente justificada por parte de los investigadores para que en su caso les ampliara el permiso.

43. Padilla, M. El kit de la lucha en internet. Traficantes de sueños ed. Madrid. 2012

44. Kleim, N. No logo. El poder de las marcas. Booket. Madrid. 2011

45. Leesing, L .El código 2.0. Traficantes de sueños (licencia Creative Commons), Madrid. 2009.

46. ¿Quién vigila al vigilante? Informe de Privacy internacional disponible en: https://www.privacyinternational.org/?q=node/351

47. La EFF haría un estudio sobre qué datos personales recopila y cómo los maneja cada una de estas empresas. Así como la forma de proceder respecto a la protección de estos o la cesión a peticiones de gobiernos y jueces: https://www.eff.org/who-has-your-back-government-data-requests-2015

48. Assange, J. Cypherpunks. La libertad y el futuro de internet. Deusto. Madrid. 2014.

49. Amy Goodman en su artículo "Ciberseguridad, criptografía y los años dorados de la vigilancia" afirma que las agencias de seguridad estadounidenses están reclamando la radica obligación legal de que las empresas estadounidenses deban permitir la existencia de "puertas traseras" para ellas:

http://www.democracynow.org/es/blog/2015/7/10/ciberseguridad_criptografia_y_los_anos_dorados otra copia en:

http://www.lamarea.com/2015/07/13/ciberseguridad-criptografia-y-los-anos-dorados-de-la-vigilancia/

El documento “Going Dark” está disponible en la página del FBI: https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy

50. Sobre cómo el GCHQ británico procede con datos sensibles:

https://firstlook.org/theintercept/2015/08/26/way-gchq-obliterated-guardians-laptops-revealed-intended/

51. El documento filtrado por WikiLeaks sobre la destrucción de equipos electronicos: https://wikileaks.org/wiki/UK_MoD_Manual_of_Security_Volu

mes 1, 2 and 3 Issue 2, JSP-
440, RESTRICTED, 2389 pages, 2001

52. El caso de Lavabit y el comunicado final de su creador dispararía todas las dudas sobre la intervención de la NSA. En su web todavía se puede ver el comunicado de este a sus usuarios:

http://lavabit.com/

53. Schneier, B. Data and Goliath .The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. 2015. Ed electrónica en: http://www.amazon.com/Data-Goliath-Battles-Capture-Control-ebook/dp/B00L3KQ1LI/

54. Sobre el comunicado de Zimmermann de su intención de marcharse de EEUU: http://www.theguardian.com/technology/2015/may/25/philip-zimmermann-king-encryption-reveals-fears-privacy

55. Listado de aplicaciones de cifrado de comunicaciones elaborado por la EFF con su catalogación respecto a diversos apartados, como la salvaguarda de la identidad, o el cifrado de mensajes: https://www.eff.org/secure-messaging-scorecard

56. El extraño mensaje que podemos ver en http://truecrypt.sourceforge.net/ , copia en: http://www.evernote.com/l/ACveegiWHfBFTKUZxzKOptAsKxJyIiUChXw/

57. La actividad en torna al soporte de la última versión fiable de TrueCrypt y la búsqueda de alternativas con bases sólidas están siendo llevadas a cabo por https://truecrypt.ch/about-us/

58. El proyecto Open Crypto Audit Project: https://opencryptoaudit.org/

59. Las conclusiones, publicadas en abril de 2015, se pueden consultar en:

http://istruecryptauditedyet.com/ y las finales en http://blog.cryptographyengineering.com/2015/04/truecrypt-report.html y en https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf

60. La asociación Pure privacy, con sede en suiza, se ha encargado de patrocinar los proyectos de cifrado de datos que sustituyan a TrueCrypt: https://pure-privacy.org/ , los proyectos derivados en: https://pure-privacy.org/projects/

61. Informe de NNUU (comisión de Derecho humanos) del 22 de mayo de 2015 sobre el derecho al cifrado: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx El documento se encuentra en: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV

62. El *Crypto Summit 2015,* pretende ser un debate abierto sobre el uso del cifrado. Sin embargo, animo a los lectores a que busquen los patrocinadores del evento para poder saber qué línea será el pivote de los debates: https://www.accessnow.org/page/content/crypto-summit/

63. La guerra del cifrado se hace global. Artículo de la EFF en el que explica la ofensiva contra el cifrado de datos de diversos gobiernos;

https://www.eff.org/deeplinks/2015/07/crypto-wars-have-gone-global

64. Reportaje de Der spieguel sobre la NSA (ingles) la clasificación de archivos y su nivel de dificultad titulado "Prying Eyes: Inside the NSA's War on Internet Security". En este, se contiene una serie de guías de la NSA sobre los métodos para romper diversos tipos de cifrado: http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html

65. El "cocinado" de tarjetas de identidad como forma de salvaguardar la privacidad frente al escaneo

https://www.washingtonpost.com/news/worldviews/wp/2015/08/14/germans-are-so-scared-of-surveillance-they-microwave-their-id-cards/ en el siguiente vídeo podemos ver el procedimiento de quemado del chip: https://www.youtube.com/watch?v=mQbfuU-6Kmg

66. Sobre la colaboración e intercambio de datos de ciudadanos alemanes con la NSA en el programa XKeyscore se ha corroborado que tan tráfico se produjo:

http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-domestic-intelligence-agency

67. Stallman, R. Software Libre para una sociedad libre. Traficantes de sueños Ed. Madrid. 2013.
Edición electrónica: http://www.traficantes.net/libros/software-libre-para-una-sociedad-libre

68. Kleim, N. La doctrina del Shock. El auge del capitalismo del desastre. Booket. Madrid. 2012

Algunas Guías en la red con aplicaciones y pautas para evadir la censura y garantizar la privacidad de comunicaciones y datos:

- La web *PRISM Break*, subministra herramientas para poder escampar de la vigilancia de sistemas como PRISM: https://prism-break.org/en/

- Seguridad Digital y Privacidad para Defensores de los Derechos Humanos, https://www.frontlinedefenders.org/esecman

- La Internacional para la Autodefensa contra la Vigilancia, https://www.eff.org/wp/surveillance-self-defense-international. En castellano: https://ssd.eff.org/es

- *Security in a Box*, será una delas primeras iniciativas para ofrecer una serie de herramientas e información sobre su uso en la salvaguarda de los derechos digitales: https://info.securityinabox.org/es

- Una guía sencilla para mantener a salvo la privacidad móvil por The Guardian Project: https://guardianproject.info/howto/

- ICCAN información sobre la infraestructura global de Internet : https://www.icann.org/es

- Herramientas básicas para navegar seguro en internet: http://andradesfran.com/10-servicios-seguros-para-resguardar-nuestra-privacidad-en-la-red/

- PRISM BREAK: Una recopilación de software para diversas plataformas para resguardarnos del espionaje masivo: https://prism-break.org/en/

- Guía de la EFF sobre privacidad y anonimato en las comunicaciones digitales: https://ssd.eff.org/es/index

- He recopilado varias guías de usuario a lo largo de mis colaboraciones con medios. Entre ellas, ha tenido mucha repercusión la dedicada a Tor y la navegación segura: http://www.eldiario.es/turing/Primeros-pasos-navegacion-segura-Tor_0_126337372.html

- La wiki sobre la censura en la red: https://en.cship.org/wiki/Main_Page

- Libro electrónico sobre la evasión de la censura en Internet por la organización
  Floss: https://howtobypassinternetcensorship.org/es.html

- Listado de aplicaciones de cifrado de comunicaciones elaborado por la EFF con su catalogación respecto a diversos apartados, como la salvaguarda de la identidad, o el cifrado de mensajes : https://www.eff.org/secure-messaging-scorecard

- Las guías de evasión de la EFF: https://ssd.eff.org/en/module/how-use-redphone-android#overlay=en/node/53/

- Una advertencia respecto a las contraseñas y su uso. L a facilidad de encortar contraseñas de productos predeterminadas hace que no cambiarlas y mantener una buena política de contraseñas sea el paso más sencillo para una intrusión.
  en http://www.phenoelit.org/dpl/dpl.html mantiene un listado de las contraseñas por defecto de gran parte de sistemas y tecnologías comerciales actuales.

- Doctorow, C. *Little Brother*. disponible en http://craphound.com/littlebrother/download/ indispensables las notas finales sobre métodos de espionaje y formas de evadirlos

V: A modo de conclusión: Una prospectiva sobre futuros posibles

En nuestro itinerario, hemos visto como Internet es una fuente de confrontación permanente entre ideas e intereses, entre legalidad, ciudadanía y libertades. La red no es aséptica ni neutral sino un territorio de conflicto. Un conflicto que se extiende a la par que la propia red se infiltra en la vida cotidiana de la ciudadanía. Una confrontación entre derechos e intereses, pero también entre libertades y restricciones. La existencia de un elemento delictivo es tan solo una parte de los peligros a los que se enfrenta la ciudadanía de nuestro tiempo. Hemos visto como en la red confluyen delincuentes, empresas y gobiernos en busca de cada vez más datos personales de una ciudadanía convertida cada vez más en espectador-consumidor. Será precisamente la capacidad de retomar su papel activo el que pueda poner un límite a este proceso. Este escenario hace inevitable el conflicto de intereses y como hemos podido ver resulta bastante sencillo rastrear estos en función al movimiento de sus partidarios.

También hemos podido ver como el poder de influencia de la gran empresa, especialmente en el entorno de Internet, ha conseguido imponer el criterio de su beneficio en diversos entornos legislativos para permitir que los márgenes de ganancia y los modelos de negocio permanezcan inalterados el mayor tiempo posible, mientras absorben o impiden la competencia real. Así, el ascenso de economías alternativas y

medios informales de acceso a la cultura ha pretendido criminalizarse hasta desfigurar la propia ley. Seguir el itinerario legislativo, especialmente en temas de derechos digitales y patentes nos ha servido para rastrear un camino en el que se evidenciaba con claridad el poder y la influencia que la gran empresa es capaz de ejercer sobre gobiernos y legisladores. Ciertos debates, oportunamente encubiertos, nos han hecho dudar acerca de los límites reales entre las prácticas del lobbies y la corrupción y han desdibujado las lindes ideológicas trazadas entre ciertos grupos que ejercen el poder en las instituciones más relevantes.

Los límites del espionaje son los que impone la tecnología. El incremento en los usos y el volcado generalizado de información por parte de la población mundial nos ha llevado a una situación en la que la exposición se ha incrementado enormemente mientras la capacidad de gestión de su propia información por parte de la ciudadanía se encuentra en un estado de escasa maduración. La confluencia de ambos factores nos ha llevado a una capacidad como nunca en la historia de la humanidad de control de la población. La inacción social, la falta de respuesta social organizada y la misma disgregación social ha propiciado el tránsito hacia una sociedad banal en la que unas redes sociales propiedad de grandes empresas estadounidenses son la fuente principal de acceso y uso de la información. La extensión de métodos de conexión mediante dispositivos móviles, ha incrementado aún más el hecho. La deriva de las actitudes críticas hacia un *clicktivismo* que no trasciende de la pose es uno de los problemas a los que se enfrenta la gestación de nuevas alternativas sociales a esta realidad.

La criminalización preventiva, significa el fracaso del concepto de sociedad democrática. Una quiebra que nos asoma a situaciones bien conocidas en la historia de nuestro país y de todo el continente europeo. El amplio provecho que la sombra del terrorismo global ha permitido a las doctrinas más restrictivas de los gobernantes de las sociedades

democráticas ha colocado en los límites de su propia definición. Ya hemos señalado cómo esta auditoría ciudadana permanente y sin garantías reales no solo es un atropello a las libertades sino una genuina declaración de intenciones de quienes desarrollan el proceso. Convertir a la red en un coto de consumo, dirigido por grandes empresas y delimitado por una legislación fuerte y un cerco policial de vigilancia permanente nos desliza peligrosamente a un futuro distópico.

Tratar de establecer una anticipación del futuro próximo es una tarea realmente complicada ante un panorama tan cambiante y lleno de posibilidades. Es un hecho que incluso autores de la llamada *ciencia ficción dura*, más realista y comprometida, están cediendo frente a otros subgéneros con menos peligro de obsolescencia. Cuando nos preguntamos cómo será el futuro que nos depara, la vista de cómo se ha organizado la economía, la sociedad y la propia red nos damos cuenta de lo difícil que es establecer la primacía de alguno de los elementos en confluencia en la red. Una de las especulaciones más sugerentes es la de la *singularidad tecnológica*. El proceso, descrito Vernor Vinge y posteriormente retomado por Ray Kurtzweill, creador del OCR (reconocimiento óptico de caracteres) y el programa de síntesis de voz que emplea el científico Richard Hawkings. El planteamiento principal sugiere que el desarrollo tecnológico llegará en un momento por precisar en el futuro próximo a que las novedades sean llevadas por una inteligencia artificial superior a la humana. Este proceso, nos llevará a un "*horizonte de sucesos*" (termino tomado de la frontera de los agujeros negros), un punto a partir del cual no seremos capaces de tener control sobre el avance posterior a cargo de una inteligencia capaz de ampliarse y por tanto desarrollarse de manera exponencial. Por supuesto, el debate estaría servido desde su comienzo y alimentaría todo tipo de suposiciones y grandes obras de la ciencia ficción, en sus versiones cinematográficas siempre distópicas. En el año 2000 se formaría el Instituto de la

singularidad y la inteligencia artificial, enfocados al desarrollo de una inteligencia artificial "fuerte". Con ello queremos exponer que nos encontramos ante un futuro muy abierto en el que factores nuevos pueden convertirse en prioritarios y establecerse como agentes de la dinámica social y económica de un futuro cercano. En el momento actual, vivimos en un momento de ruptura de la confianza hacia gobiernos y empresas vinculadas a la red. La evolución de este proceso hacia formas de defensa de la privacidad y la intervención en los mecanismos y fuentes de este poder pueden significar un cambio completo de la línea actual de nuestra sociedad.

La capacidad de dirección democrática del futuro que viene, de retomar el peso social y reconstituir la soberanía ciudadana, en un entorno en el que esta adelgaza, puede ser la cuestión principal de todo proceso que hemos narrado en todo el presente trabajo. El software libre, la nueva visión de los derechos de autor, las formas de consumo responsable y a escala y la toma de control de dispositivos y elementos tecnológicos que pueblan nuestra cotidianidad, son factores que apuntan a una forma diferente de trazar el futuro de la tecnología y la red. La disyuntiva entre comodidad y uso cediendo privacidad es una responsabilidad que debería ser prioritaria tanto entre usuarios como entre desarrolladores.

Cuando iniciamos este trabajo, citábamos la dicótoma en la que nos sitúa nuestro presente. La pormenorizada exposición de los hitos destacados en el desarrollo del Internet de nuestros días y su constante cruce transversal con el de la misma sociedad nos llevan al punto de elevar nuestra reflexión sobre cómo se han sucedido los últimos tiempos. La dirección que estos cambios están tomando es producto de una visión doctrinaria de la econonomía y la sociedad. El viejo enunciado de Thatcher sobre que no hay alternativa es un meditado paralogismo. Por ello, una vez

expuesto nuestro análisis no podemos más que concluir que seguimos optando por la pastilla roja.

Sobre el método de trabajo:

He tratado de recopilar todos los enlaces posibles priorizando el castellano. Asimismo, he mantenido todo el apoyo bibliográfico posible, aunque algunos de los temas tratados son tan actuales que apenas podemos encortar documentación solvente que no tenga origen en el propio Internet o publicaciones periodísticas. En esos casos se han buscado fuentes de reconocida solvencia, con datos suficientemente objetivables o argumentos contrastados.

Como herramienta de trabajo principal he empleado la aplicación *Evernote*, que me ha permitido mantener actualizados los contenidos prácticamente hasta el cierre definitivo previo a su impresión. Este trabajo utiliza eminentemente los enlaces y por tanto, he optado por mantenerlos en su versión digital, para poder seguirlos con mayor facilidad. Todos los enlaces que contiene el presente trabajo han sido revisados en septiembre de 2015 y en esa fecha todos devolvían un resultado correcto. No obstante, tanto con la aplicación *Evernote* como con *Pocket*, mantengo copias de las referencias para poder recuperarlas en caso de que esos enlaces se rompieran. El formateado final del texto se ha realizado con la versión 5 de Libre Office.

Incluso en la Bibliografía, he preferido dar prioridad a las versiones digitales sobre las editadas en papel. Muchas de las obras referenciadas

en este trabajo cuentan con licencias Creative Commons u otras de igual carácter. Por ello he optado por posibilitar el acceso a estas para su contrastado y ampliación. Con el tiempo, Internet a permitir el acceso a obras que de otro modo resultaría difícil logar, incluso no disponibles en nuestro país.

En lo que respecta a la línea de tiempo, hemos procurado seguir un itinerario temporal en la disposición de nuestros capítulos. Los dos primeros bloques lo siguen con exactitud. Sin embargo, los dos siguientes tratan sobre temáticas más concretas y en muchos casos se solapan. Así podrá verse como ciertos elementos son referenciados en diversos capítulos del trabajo. Los dos últimos bloques, más enfocados a legislación y cultura y a conflicto y activismo respectivamente, no siguen con tanta exactitud dicha premisa. También se trata de los capítulos con más densidad y extensión al tratar directamente los temas sobre los que se fundamenta la tesis en sí misma.

En los capítulos que hacen referencia a momentos más recientes, mantener las formas de crónica histórica se hace más complicado. A la hora de explicar momentos concretos o desarrollos de software y la influencia que estos pueden tener, por poner un ejemplo, estamos tratando de cuestiones de completa actualidad, que todavía no han trazado su arco "histórico" completo y por tanto no podemos cerrar. En estos, hemos optado por la descripción y valorar la influencia que pueda tener.

Respecto a la adopción y normalización de neologismos en este trabajo hemos tenido que optar por el compromiso de su empleo. Por tanto, hemos optado por obviar un entrecomillado que llevaría al exceso. Para mejorar la compresión, se ha tratado en todo momento de emplear los términos técnicos solo cuando no existía una alternativa clara en castellano. De cualquier modo, en todos los casos hemos acudido a la

explicación entre paréntesis en lugar del pie de página o la referencia en glosarios, dado que ambas alternativas serán, a nuestro criterio, formas de ralentizar la lectura y dificultar la compresión del trabajo. En este tipo de publicaciones, o al menos en lo que a las de corte periodístico que ha realizado en su labor profesional por parte del que escribe, siempre se ha jugado en un delicado equilibrio entre la precisión de las explicaciones o la concisión y facilidad comprensiva. Desde ambos extremos siempre es posible la crítica, pero en esta ocasión se ha optado por un equilibrio calculado y la opción de ampliar en una profusión de notas al pie llenas de enlaces lo más actualizados que ha sido posible. Cualquiera de los temas aquí propuestos, pueden ser ampliados y de hecho se ha realizado un importante ejercicio de resumen y concisión, dado que lo importante es fijar una perspectiva general del asunto, contando con las caras que componen esta figura papirofléxica de la que está formada la realidad de la red.

VI. Bibliografía

- Alberganti, M. *Los Microprocesadores contra las libertades*; en El estado del Mundo 2009. Akal. Barcelona. 2008

- Assange, J. *Cypherpunks. La libertad y el futuro de internet*. Deusto. Madrid. 2014.

- Assange, J. *Cuando Google encontró a WikiLeaks*. LMD-Clave Intelectual. Madrid. 2014

- Augé, M. *Sobremodernidad: del mundo tecnológico de hoy al desafío esencial del mañana.* En Sociedad Mediatizada. Gedisa. Barcelona.2007.

- Arquilla. J y Ronfeld D. *Network and Netwars. The Future of Terror, Crime and Militancy.* Rand. Santa Mónica. 2014. Una copia en formato electrónico disponible en: http://www.rand.org/pubs/monograph_reports/MR1382.html#download

- Banford, J. *The Most wanted man in the world*. Wired. 2014. Recurso disponible en: http://www.wired.com/2014/08/edward-snowden/#ch-1

- Barandiaran, X. *Activismo digital y telemático. Poder y contrapoder en el ciberespacio*. 2003. Recurso disponible en http://www.sindominio.net/~xabier/textos/adt/adt.html

- Barceló, M. *Una Historia de la informática*. UOC ed. Barcelona. 2008

- Bell, Daniel. *El Fin de las ideologías: sobre el agotamiento de las ideas políticas en los años 50*. MTyAS. Madrid. 1992.

- Blum, A. Tubos. *En busca de una geografía física de Internet*. Océano Ed. Barcelona. 2013

- Bravo, D. *Copia Este libro*. Dolmen. Madrid. 2005. Disponible en http://elastico.net/archives/005194.html y en http://copiaestelibro.bandaancha.st/

- Brockam, J. *La tercera Cultura. Más allá de la revolución científica*. Tusquets. Barcelona. 1996.

- Bustamante, E. *Hacia un nuevo sistema mundial de comunicación: las industrias culturales de la era digital*. Gedisa, Barcelona, 2004

- Brzezinski, Z. *La Era tecnotrónica*. Paidós, Buenos Aires, 1979

- Castells. M, *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*. Plaza & Janes. Barcelona. 2001

- Castells, M. *Innovación, libertad y poder en la era de la información.* En Sociedad Mediatizada. Gedisa. Barcelona, 2007.

- Castells, M. *La era de la información: economía, sociedad y cultura (Vol. 1):* La sociedad red. Alianza editorial. Madrid. 2008

- Castells, M. *La era de la información: economía, sociedad y cultura (Vol. 3)*: .Fin del milenio. Alianza editorial. Madrid. 2008

- Castells, M. *Comunicación y poder*. Alianza Editorial. Madrid. 2009.

- Chomsky, Noam. *El control de los medios de comunicación*. Icaria. Barcelona. 2008

- Chomsky, Noam. *Ilusiones necesarias. Control del pensamiento en las sociedades democráticas*. Libertarias/Prodhufi. Madrid.1992

- Cline, E. *Ready Player one.* Ediciones B. Barcelona. 2011.

- Cobo, C. y Pardo H*. Planeta Web 2.0. Inteligencia colectiva o medios fast food*. Grup de Recerca d'Interaccions Digitals, Universitat de Vic. Flacso México. Barcelona / México DF. ,2007. también disponible en: http://www.planetaweb2.net/

- Craig, T y Ludloff, M. *Privacy and Big Data. The Players, Regulators, and Stakeholders*. O'Reilly Media. Massachusetts. 2011

- Dans, E. *Todo va a cambiar. Deusto*. Madrid. 2010

- Dawkins, R. *El capellán del diablo*. Gedisa. Barcelona. 2005.

- De la Cueva, J. *Propiedad intelectual, nuevas tecnologías y libre acceso a la cultura.* 2008. Libro con licencia Creative Commons disponible en: http://radio-ccemx.org/descargas/propiedadint.pdf

- Dirscherl, K, Bernecker, L. *Spanien heute. Politik, Wirtschaft, Kultur.* Frankfurt/M. 2004

- Dirscherl, K, Bernecker, L (coords) Posdictadura/posmodernismo La renegociación de identidades colectivas en la España democrática: entre memoria histórica, cultura popular y cultura política. 2004. Artículo disponible en http://journals.iai.spk-berlin.de/index.php/iberoamericana/article/download/645/329

- Dirschel, Klaus: “Poesía bajo Franco: Jaime Gil de Biedma entre compromiso y juego intertextual”. Actas del X Congreso de la Asociación Internacional de Hispanistas, Barcelona 21-26 de agosto de 1989, 1992

- Doctorow, C. *Little Brother*. disponible en http://craphound.com/littlebrother/download/

- Dromscheit-Berg, D. *Dentro de WikiLeaks. Mi etapa en la web más peligrosa del mundo.* Roca. Barcelona. 2011

- Ensmenger, N. L. *The Computer Boys Take Over*. The MIT Press. 2010

- Echeverría, J. *Los señores del aire. Telépolis y tercer entorno*. Destino. Barcelona. 1998

- FMI. *La globalización ¿amenaza u oportunidad?* : http://www.imf.org/external/np/exr/ib/2000/esl/041200s.htm

- García, C. y Arroyo D. *Biblioteca Digital y Web Semántica*. disponible en: http://biblioweb.sindominio.net/telematica/bibdigwebsem.html

- García Galindo, Juan Antonio*: “Análisis de la información internacional en la prensa digital española/Analysis of international information in Spanish digital.*” *Estudios Sobre el Mensaje Periodistico*, 01/2014, Volumen 20, Número 1

- Garzón, A. *La gran estafa*. Península. Barcelona 2013.

- Gastesi, M y Creus, D*. Fraude online. Abierto 24 horas*. 0xWorld. Madrid. 2013

- Gibson, Wiliam. *Neuromancer*. Minotauro. Barcelona.1989.
- Gillmor, D. *Nosotros el medio. 2004*. Libro disponible con licencia Creative Commons
  en: http://www.hypergene.net/wemedia/espanol.php
- González Pérez, P. *Ethical Hacking*.0xWorld, Madrid. 2014
- Gramsci, Antonio. *Cuadernos de la Cárcel*. Ediciones Era. México. 1981
- Greenwald, Glenn - *Snowden. Sin un lugar donde esconderse*. Ediciones B. Barcelona. 2014
- Herrera León, B. El modelo UNESCO de comunicación en el «Informe MacBride». *Anuario Inicio*, jun. 2005, vol.17, no.1
- Harnecker, M. *Haciendo posible lo imposible. La izquierda en el umbral del siglo XX.*l Siglo XXI, Madrid, 2000.
- Herrera León, B*. El modelo UNESCO de comunicación en el «Informe MacBride».* Anuario Inicio, jun. 2005, vol.17, no.1
- Himanen, P. *La ética del hacker y el espíritu de la era de la información.* Destino. Barcelona. 2004
- Isaacson, W. *Steve Jobs*. Trinith & Banshee. NY. 2011
- Jones, O. Chavs. *La demonización de la clase obrera*. Capitán Swing. Madrid. 2012
- Kleim, N. *La doctrina del Shock*. El auge del capitalismo del desastre. Booket. Madrid. 2012
- Kleim, N. *No logo. El poder de las marcas*. Booket. Madrid. 2011

- Lanier, J. *Contra el rebaño digital: Un manifiesto*. Debate. Barcelona. 2011

- Lessig.L. *El código 2.0*. Traficantes de sueños (licencia Creative Commons), Madrid. 2009.

- Lessig.L. *Por una Cultura libre. Cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad*. LOM. Santiago, 2005. Edición electronica: http://www.traficantes.net/libros/por-una-cultura-libre

- Lessig.L Remix. *Cultura de la remezcla y derechos de autor en el entorno digital*. Icaria. Barcelona 2011

- López Ocón Cabrera, Leoncio; Díaz Mas, Miguel; Alonso, María Soledad: *"De ultramar a internet: experiencias investigadoras y divulgativas del patrimonio de la Comisión Científica del Pacífico*". *Historia de las ciencias y de las técnicas*, Universidad de La Rioja 2004, 229-244

- Lyotard. J.f. *La Condicion Postmoderna. Informe sobre el saber*. Planeta. Barcelona. 1979

- Echeverría, J.*: Los Señores del aire: Telépolis y el Tercer Entorno*. Barcelona (Destino) 1999

- Marcuse, Herbert. *El hombre unidimensional*. Ariel. Barcelona. 1994

- Matterart, A .*Historia de la sociedad de la información*. Paidós, Barcelona. 2007

- Matterland, A. *¿Hacia qué "Nuevo Orden Mundial de la Información"?. En Sociedad Mediatizada*. Gedisa. Barcelona, 2007.

- Materland, A. *La información contra el estado*. Le Monde Diplomatique , nº 21 Marzo 2001
- McLuhan, M. *La galaxia Guttember: génesis de homo tipographicus*.Círculo de lectores, Barcelona. 1998.
- McLuhan, M. *La Aldea Global*. Gedisa. Barcelona. 2005
- McBride, S y otros. *Un solo mundo. Voces múltiples. Comunicación en información en nuestro tiempo*. Fondo de Cultura Económica y UNESCO. México, 1980. Disponible en: http://unesdoc.unesco.org/images/0004/000400/040066sb.pdf
- Metzner-Szigeth, A.: "*El movimiento y la matriz" – Internet y transformación socio-cultural*. En: Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación (CTS+I), No. 7, 2006
- Mitnick, K.D. *El Arte de la Intrusión*. Ra-Ma. Madrid. 2006
- Molist, M. *Hackstory.es. las historia nunca contada del underground hacker en la península ibérica*. 2014. Disponible en formato electrónico en : http://hackstory.es/
- Morales Muñoz, Manuel: *Propaganda doctrinal y difusión de la prensa internacionalista (1869-1873)* Baetica, 01/1989, Volumen 12, Número 12.
- Mounier, Pierre. *Las nuevas tecnologías de la información y la crisis de la cultura*; en El estado de Mundo 2009. Akal. Barcelona. 2008
- Naciones Unidas. *IDH-Año 2004. Libertad Cultural y desarrollo Humano.* Ediciones Mundo-Prensa, 2004

- Padilla, M. *El kit de la lucha en internet*. Traficantes de sueños ed. Madrid. 2012

- Paterson, T*. From the Mailbox: The Origins of DOS:* http://www.ece.umd.edu/courses/enee759m.S2000/papers/paterson1994-kildall.pdf

- Peña, R. *Cuadernos de consultor para el curso de hacking ético*. UDIMA. Madrid. 2015

- Pérez, C. *Las nuevas tecnologías: Una visión de conjunto. En La tercera revolución industrial (Impactos internacionales del nuevo viraje tecnológico)*. Rial, Buenos Aires. 1986.

- Periano, M. *El pequeño libro rojo del activista en la red*. eldiario.es libros. Madrid. 2015

- Piketty, T. *La crisis del capital en el siglo XXI. Crónicas de los años en que el capitalismo se volvió loco*. Siglo veintiuno editores. Buenos Aires. 2014.

- Preuss-Laussionotte, S. *La democracia ante los riesgos de la mundialización de las bases de datos*. En El estado del mundo 2009. Akal, Barcelona 2008.

- Ramonet, I (Ed.) (1998): *Internet, el mundo que llega*. Madrid, Alianza.

- Ramonet, I. *Pensamiento único y nuevos amos del mundo*. Icaria. Barcelona. 2008

- Ramonet, Ignacio. *El control de Internet. en* Le Monde Diplomatique*, 04/11/05*. También disponible en http://www.insumisos.com/diplo/NODE/898.HTM

- Ramonet, I. "*Nouveau pretê-á-penser ideologique*". Le Monde Diplomatique, Mayo- 1992
- Ramos Santana, Alberto: *Una historia de los cursos de verano en Andalucia: monografía histórica*. Observatorio Atalaya, 2009
- Rebillard Franck. *De OhmyNews a Meidapart: ¿un nuevo modelo de periodismo?* ; en El estado de Mundo 2009. Akal. Barcelona. 2008
- Reischl, G. *El engaño de Google*. Medialive Content. Barcelona. 2008
- Rifkin, J. *El fin del trabajo. Nuevas tecnologías contra puestos de trabajo: El nacimiento de una nueva era*. Paidós. Barcelona. 2004
- Rodríguez, D. *Ceros y Unos: La increíble historia de la informática.* Ciudadela Libros. Madrid. 2011
- Rojas, Raúl (1998). *«How to make Zuse's Z3 a universal computer»* IEEE Annals of the History of Computing (documento completo en: http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=707574#)
- Sánchez de Almeida, C. *República Internet. Un libro en formato Blog (hasta julio de 2013)* http://republicainternet.com/
- Serrano, A y Martínez; E. *La Brecha Digital: Mitos y Realidades*, Editorial UABC, México, 2003, Disponible en : www.labrechadigital.org

- Schönberger, V. Big Data: *A Revolution That Will Transform How We Live, Work, and Think.* Hougton Mifflin Harcourt. Nueva York. 2013

- Schneier, B. *Data and Goliath .The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company. 2015 Ed electrónica en http://www.amazon.com/Data-Goliath-Battles-Capture-Control-ebook/dp/B00L3KQ1LI/

- Suárez Sánchez Ocaña, A. *Desnudando a Google*. Deusto. Madrid. 2012

- Stallman, R. *Software Libre para una sociedad libre*. Traficantes de sueños Ed. Madrid. 2013. Edición electronica: http://www.traficantes.net/libros/software-libre-para-una-sociedad-libre

- Stallman y otros. *Contra el Copyright*. Tumbona Ediciones. México. 2008. Edición electrónica: http://bibliotecalibre.org/handle/001/352

- Stephenson, N. *En el principio fue la línea de comandos*. Traficantes de sueños (ed). Madrid. 2003

- *Stephenson, N.Snow crash. Gigamesh. Barcelona. 2008*

- Ugarte de, D. *Filés: De las naciones a las redes*. Colección Biblioteca de las Indias. Madrid. 2008

- Ugarte de, D. *Los futuros que vienen*. Colección Biblioteca de las Indias. Madrid. 2010

- Ugarte de, D. *El poder de las redes*. Colección Biblioteca de las Indias. Madrid. 2011

- VVAA. *Capitalismo cognitivo, propiedad intelectual y creación colectiva*, Traficantes de

sueños.Madrid:(2004) En: http://sindominio.net/traficantes/editorial/capitalismocognitivo.htm

- VV.AA. *Echelon. La red de espionaje planetario*. Melusina. Barcelona. 2007
- VVAA. *Manifiesto Cluerain http://www.cluetrain.com/* TESIS EN CASTELLANO http://tremendo.com/cluetrain/ . 1999.
- VVAA. *Informe de Amenazas CCN-CERT IA-09/15 Ciberamenazas 2014 y Tendencias 2015.* Centro Criptológico Nacional. Madrid. 2015
- VVAA. *Guía de seguridad del las TIC CCN-STIC-817. Esquema Nacional de Seguiridad. Gestión de Ciberincidentes.* Centro Criptológico Nacional. Madrid. 2015
- VVAA. *Internet y Lucha política: Los movimientos sociales en la red.* Capital Intelectual, Buenos Aires, 2006
- VVAA.(Fundación Telefónica). *La Sociedad de la Información en España 2006*. Ariel. Madrid.http://www.telefonica.es/sociedaddelainformacion/pdf/sociedaddelainformacion2006.pdf
- VV.AA. *Sociedad Mediatizada*. Gedisa. Barcelona.2007
- VVAA. *Pentesting con Kali*. 0xwolrd. Madrid. 2014
- VVAA. *The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008), ISBN 0-262-54196-3 http://www.opennet.net/accessdenied/
- VVAA. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), ISBN 0-262-51435-4 http://www.access-controlled.net

- VVAA. *CopyLeft. Manual de uso*. Traficantes de sueños. Madrid. 2006. Recurso con licencia *Creative Commons* también disponible en: http://www.articaonline.com/wp-content/uploads/2011/07/Copyleft-Manual-de-uso.pdf

- VVAA. *Cultura Libre Digital*. Icaria. Barcelona. 2012

- VVAA. *Cultura digital y movimientos sociales*. Catarata. Madrid. 2008

- VVAA: *Circumvention Tool Usage Report*. Harvard University. Massachusetts. 2010. Disponible en : http://cyber.law.harvard.edu/publications/2010/Circumvention_Tool_Usage

- VVAA. *Geopolítica del caos*. Debate. Madrid. 1999

- VVAA. *Los Piratas son los padres.* Traficantes de Sueños. Madrid. 2008

- VVAA. *Pásalo. Relatos y análisis sobre el 11M y los días que siguieron.* Traficantes de sueños. Madrid. 2014

- VVAA. *Tus derechos en el trabajo*. Lulu Press. Morrisville. 2014

- Vitalliev, D. *Seguridad y privacidad digital para los defensores de los derechos humanos*. Front Line Foundation. 2009. *Recurso disponible en la web con licencia Creative Commons*

- Wallernstein, I. *Geopolítica y Geocultura. Ensayos sobre el moderno sistema mundial*. Kairós, Barcelona, 2007.

- Wiener, N. *Dios y Golem S.A.* Lestrobe (edición digital) 2014

- Wattson, P. *Historia intelectual del siglo XX*. Crítica. Barcelona. 2012

- Wu Ming. *Contra el Copyright. 2008*. Recurso disponible en: http://www.tumbonaediciones.com/vs-copyright.pdf y en http://www.wumingfoundation.com/italiano/spanish_directo.htm#2003

Recursos en Internet

- Glosario de siglas y nombres de internet : http://www.rfc-es.org/guia/glosario-siglas.txt
- Otro glosario muy detallado sobre internet : http://www.internetglosario.com
- Gráficos sobre la evolución de microprocesadores
    - http://www.network-press.org/?que_es_microprocesador
    - http://www.intel.com/products/processor_number/chart/
    - http://www.youtube.com/watch?v=trBZXWIX8Zk&feature=related
- Traducciones a castellano de toda la documentación relativa a protocolos y estándares de red e Internet en general: http://www.rfc-es.org/
- CNN_CERT (Centro Criptológico Nacional) Perteneciente al gobierno de España. Presenta al público algunos de sus informes sobre seguridad, amenazas y gestión de recursos en el Internet español. https://www.ccn-cert.cni.es/
- Akamai: informe anual sobre el estado de internet.

- Freedom House: Informes sobre la libertad y la censura en Internet
- Kaspersky Labs: la Página Securelist ofrece informes sobre seguridad e incidentes en la red muy interesante y actual.
- Manuales contra la censura: http://en.flossmanuals.net/bypassing-es/ disponibles en epub y pdf http://en.flossmanuals.net/_booki/bypassing-es/bypassing-es.epub http://en.flossmanuals.net/_booki/bypassing-es/bypassing-es.pdf
- Reporteros sin fronteras, *Manual de Blogueros y Ciberdisidentes,* http://www.rsf.org/article.php3?id_article=26187
- La Wiki de la Censura en Internet, http://en.cship.org/wiki/
- La Caja de recursos para ONG, una colección de aplicaciones y tutoriales para hacer un uso seguro de la red, https://security.ngoinabox.org
- Seguridad Digital y Privacidad para Defensores de los Derechos Humanos, https://www.frontlinedefenders.org/esecman
- La Internacional para la Autodefensa contra la Vigilancia, https://www.eff.org/wp/surveillance-self-defense-international
- Una guía sencilla para mantener a salvo la privacidad móvil por The Guardian Project: https://guardianproject.info/howto/
- ICCAN información sobre la infraestructura global de Internet : https://www.icann.org/es
- Herramientas básicas para navegar seguro en internet: http://andradesfran.com/10-servicios-seguros-para-resguardar-nuestra-privacidad-en-la-red/

- *PRISM BREAK*: Una recopilación de software para diversas plataformas para resguardarnos del espionaje masivo: https://prism-break.org/en/

- Guía de la EFF sobre privacidad y anonimato en las comunicaciones digitales: https://ssd.eff.org/es/index

- La Metabiblioteca: Libros de acceso abierto: http://bibliotecalibre.org

- He recopilado varias guías de usuario a lo largo de mis colaboraciones con medios. Entre ellas, ha tenido mucha repercusión la dedicada a Tor y la navegación segura: http://www.eldiario.es/turing/Primeros-pasos-navegacion-segura-Tor_0_126337372.html

- Guía para conocer y gestionar recursos en la Criptomoneda Bitcoin: https://bitcoin.org/es/

- Freenet. Una red segura, prácticamente imposible de rastrear: https://freenetproject.org/index.html

- La wiki sobre la censura en la red: https://en.cship.org/wiki/Main_Page

- Libro electrónico sobre la evasión de la censura en Internet por la organización Floss: https://howtobypassinternetcensorship.org/es.html

- El proyecto TOR, es la web donde se suministran las herramientas para acceder a la red oculta más famosa de nuestros tiempos: https://www.torproject.org

- *The Hidden Wik*i, es el portal de acceso desde la web convencional que nos suministra una serie de enlaces a la red oculta. Es

conocida como la puerta de entrada más famosa a los servicios ocultos http://thehiddenwiki.org/ . su versión oculta y sin censura está disponible en: http://zqktlwi4fecvo6ri.onion/

- *Grams*, es uno de los buscadores más recientes y que mejores resultados ofrecen en la búsqueda de mercados ilegales en la web oculta. Su funcionamiento, muy parecido al de Google en la web convencional, lo hace sencillo y fácilmente reconocible en todos sus servicios : http://grams7enufi7jmdl.onion/

Gráficas, estadísticas e informes sobre Internet

- *Internet World Stats*: Estadísticas mundiales sobre Internet : http://www.internetworldstats.com/
- Sobre GNU y las categorías de código abierto existentes: http://www.gnu.org/philosophy/categories.es.html#CopyleftedSoftware
- G.E. Moore. "*Progress in digital integrated electronics*", IEEE International Electron Devices Meeting, IEDM Technical Digest 1975, pp. 11-13
- Página de la CIA sobre acceso a internet y otras tablas estádísticas: https://www.cia.gov/library/publications/the-world-factbook/rankorder/2153rank.html
- W3ounter: Estadísticas globales sobe internet: http://www.w3counter.com/globalstats.php
- INE: http://www.ine.es/
- Instituto Internacional de estadística http://isi.cbs.nl/

- INE: encuesta de condiciones de vida(actualizado a 2014) http://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176807&menu=ultiDatos&idp=1254735976608

- OIT, estadísticas sobre el empleo: http://www.ilo.org/global/What_we_do/Statistics/lang--es/index.htm

- Informes de la Comisión europea (EUROSTATS) sobre la productividad de la mano de obra: http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tsieb040

- EUROSTAT: http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home

- Gráficas de acceso a Internet en Europa : http://epp.eurostat.ec.europa.eu/tgm/mapToolClosed.do?tab=map&init=1&plugin=1&language=en&pcode=tsiir040&toolbox=legend

- Naciones Unidas. Todos los Índices de Desarrollo Humano: http://hdr.undp.org/es/informes/mundial/

- Especificaciones del HTTP del W3 consortium http://www.w3.org/Protocols/

- sobre el monopolio de AT&T http://morfeo.upc.es/crom/mod/wiki/view.php?id=4&page=view/Monopolio+de+AT&editor=dfwiki&gid=0&uid=0

- Distribución de los servidores dns raíz por el mundo : http://norfipc.com/infografia/mapa-mundial-redes-conexion-internet.html

- Expansión de la IPv6 : https://www.icann.org/news/blog/ipv6-a-montones

- UIT: (Unión internacional de Telecomunicaciones- ITU en inglés) datos sobre la penetración de internet en el mundo en el periodo 2000-2015 https://www.itu.int/net/pressoffice/press_releases/2015/17-es.aspx

- UIT: Estadísticas sobre la evolución de internet en el periodo 2000-2015: https://www.itu.int/net/pressoffice/press_releases/2015/17-es.aspx

- UIT : Porcentajes de uso individual de Internet por países http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

- España Conecta. La transformación dela economía española a través de Internet: http://www.espanaconecta.es/informe/ (patrocinado por Google y The Boston Consulting Group- BCG)

- INE. Informe sobre el impacto de la lectura digital en España: http://www.ine.es/ss/Satellite?L=es_ES&c=INECifrasINE_C&cid=1259932520217&p=1254735116567&pagename=ProductosYServicios%2FPYSLayout

- *Informe Global eBook 2015*. Un documento de Rüdiger Wischenbart, en el que se detalla el estado internacional del mercado del libro electrónico: http://www.global-ebook.com/

- Informe de la Asociación de telecomunicaciones británica sobre la seguridad y el coste del monopolio en las grandes redes. Sobre todo hace mención al peligro para la seguridad del monopolio de

Microsoft *CyberInsecurity: The Cost of Monopoly* : http://cryptome.org/cyberinsecurity.htm

- EUROSTAT: Cifras de uso de Internet móvil : http://ec.europa.eu/eurostat/help/new-eurostat-website?p_auth=jVcHEUXV&p_p_id=estatsearchportlet_WAR_estatsearchportlet&p_p_lifecycle=1&p_p_state=maximized&p_p_mode=view&_estatsearchportlet_WAR_estatsearchportlet_action=search&text=Individuals+using+a+mobile+phone+via+UMTS+%283G%29+to+access+the+internet

- Tendencias internacionales 2015 del mercado de las comunicaciones móviles : http://www.budde.com.au/Research/Global-Mobile-Communications-Market-Insights-Statistics-and-Regional-Trends.html

- informe de la agencia We are social sobre el impacto del intercambio de información y las comunicaciones a través de redes sociales 2015 nos ubica en la realidad de las redes sociales en nuestro tiempo: http://wearesocial.sg/blog/2015/01/digital-social-mobile-2015/

- Estudio de Nielsen sobre el uso del Smartphone: http://www.nielsen.com/us/en/insights/news/2015/so-many-apps-so-much-more-time-for-entertainment.html

- *Las cifras del porno*. Estadísticas anuales (2014) del portal *PornHub*, uno de los mayores del mundo, sobre usos y accesos a sus contenidos: http://www.pornhub.com/insights/2014-year-in-review

- *La neutralidad de la red en Europa*. Una infografía interactiva (tipo línea de tiempo) en la que se detallan los eventos más importantes

al respecto de la neutralidad de la Red: http://www.tiki-toki.com/timeline/entry/108784/Net-neutrality-in-Europe/#vars!date=2010-01-04_21:35:39!

- Listado de sistemas de vigilancia masiva internacional mantenida por la fundación Wikipedia: https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects

- Privacy Internacional y Amnistía internacional han publicado un informe sobre el estado de la cuestión de las revelaciones de Edward Snowden titulado "*Two Years after Snowden. Protecting Human Rights in an age of mass surveillance"*. Disponible en : https://www.privacyinternational.org/?q=node/591

- Informe sobre la adquisición de datos biométricos y su gestión a cargo de Privacy International: https://www.privacyinternational.org/?q=node/48

- Informe anual de la empresa de seguridad TrendMicro sobre las tendencias del ciberdelito: http://www.trendmicro.es/newsroom/pr/el-informe-anual-de-seguridad-de-trend-micro-revela-que-el-ataque-a-sony-en--increment-el-cibercrimen-y-la-proliferacin-de-ransomware/

- *Informe anual de la empresa de seguridad Symantec sobre las amenazas para la seguridad en Internet*, 2015:http://www.symantec.com/es/es/security_response/publications/threatreport.jsp

- *Estrategia Europea de ciberdefensa* (diseñada a lo largo de 2013 y puesta en marcha en 2014: http://www.eda.europa.eu/info-hub/news/2015/07/13/military-requirements-for-cyber-ranges-agreed

- EL Real Instituto Elcano, en colaboración con THIBER (the Ciber security Think thank) mantiene una serie de informes mensuales sobre ciberseguridad en los que colaboran los más destacadas personalidades del sector. Los informes está disponibles en http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/publicaciones/ciber-elcano/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP0os3jjEBf3QG93QwMLQwNLA0dfD7PAwABXI-8QI_2CbEdFAMWyODY!/

- THIBER (The Ciber security Think thank) es una organización que se encarga de difundir la importancia de estrategias de ciberseguridad entre gobiernos y empresas. Mantienen en su sitio una recopilación de artículos e informes al respecto muy interesante disponible en: http://www.thiber.org/articulos/

- CNN- CERT (Centro Criptológico nacional- Gobierno de España) *Informe de ciberamenazas 2014 y tendencias 2015.* recurso disponible en: https://www.ccn.cni.es/index.php?option=com_content&view=article&id=18&Itemid=22

- CNN- CERT (Centro Criptológico nacional- Gobierno de España): Guías del esquema Nacional de Seguridad: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

- Graficas sobre ataques y cargas de Internet a nivel mundial http://www.akamai.com/html/technology/dataviz1.html

- *Guía de pasos para la OSINT* (tareas de Inteligencia a nivel navegador) para realizar una investigación desde la propia red con los datos que pueden extraerse de esta sobre individuos y organizaciones. http://onstrat.com/osint/

- Mapa global del estado de la "ciberguerra" a escala mundial: http://cybermap.kaspersky.com/

- Otro mapa interactivo sobre guerra digital : http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=16601&view=map

- La empresa de seguridad Fireeye cuenta con otro mapa de ataques declarados en la red en tiempo real: https://www.fireeye.com/cyber-map/threat-map.html

- Estrategias de ciberseguridad en el mundo http://www.thiber.org/estrategias-nacionales-de-ciberseguridad-en-el-mundo/

- Informe de NNUU (comisión de Derecho humanos) del 22 de mayo de 2015 sobre el derecho al cifrado: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx El documento se encuentra en: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

- Informe de la sección de ciberseguridad de la BSA sobre Europa y las diferentes estrategias de seguridad nacional a lo largo de 2015: http://ww2.bsa.org/country.aspx?sc_lang=es-ES

- Informes de transparencia de las tres grandes empresas propietarias de redes sociales:

    - Google: https://www.google.com/transparencyreport/?hl=es

    - Facebook: https://govtrequests.facebook.com/

    - Twitter: https://transparency.twitter.com/

- Informe de la UNESCO sobre la censura de internet. *Freedom of Connection, Freedom of Expression,* disponible en: Freedom of Connection, Freedom of Expression".

- Los mapas de Open Net nos muestran los niveles de censura y filtrado de Internet en el mundo. Para el caso egipcio, puede consultarse el histórico: http://map.opennet.net/

- *¿Quién vigila al vigilante?* Informe de Privacy internacional disponible en : https://www.privacyinternational.org/?q=node/351

- Informe de Reporteros Sin Fronteras. *"Enemigos de Internet 2014: organismos en el epicentro de la censura y la vigilancia":* http://www.rsf-es.org/news/rsf-publica-el-informe-enemigos-de-internet-2014/

- La EFF haría un estudio sobre qué datos personales recopila y cómo los maneja cada una de estas empresas. Así como la forma de proceder respecto a la protección de estos o la cesión a peticiones de gobiernos y jueces: https://www.eff.org/who-has-your-back-government-data-requests-2015

- Informe completo sobre los mercados de la ciberdelincuencia en el mundo por parte de trend Micro. El informe recopila tres grandes estudios sobre las zonas de Rusia, China y Brasil, junto con un análisis de precios de servicios y formas de venta de estos: http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/

- Informe de Reporteros Sin Fronteras. "*Enemigos de Internet 2014: organismos en el epicentro de la censura y la vigilancia*": http://www.rsf-es.org/news/rsf-publica-el-informe-enemigos-de-internet-2014/

- LA IPI (International Press Institute) ha elaborado un documento sobre el cifrado y el anonimato en la red, titulado "Special report: Encryption, anonymity as safeguards for press freedom" explicado en :https://www.ifex.org/international/2015/08/21/encryption_anonymity/?i=1 y disponible en http://ontheline.freemedia.at/special-report-encryption-and-anonymity/

- ¿Quién vigila al vigilante? Informe de Privacy internacional disponible en : https://www.privacyinternational.org/?q=node/351

- Reportaje de Der spieguel sobre la NSA (ingles) la clasificación de archivos y su nivel de dificultad titulado "Prying Eyes: Inside the NSA's War on Internet Security". En este, se contiene una serie de guías de la NSA sobre los métodos para romper diversos tipos de cifrado: http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html

Medios de Comunicación y cultura

- Observatorio Internacional de Medios: http://www.mwglobal.org/

- OIT, estadísticas sobre el empleo: http://www.ilo.org/global/What_we_do/Statistics/lang--es/index.htm

- informe del parlamento europeo sobre echelom http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_es.pdf

- Statewach. Una web que recoge publicaciones sobre libertades cívicas en Europa. Muy interesante su labor de vigilancia y

recopilación de toda la actividad europarlamentaria en los aspectos de libertades y vigilancia ciudadana.: http://statewatch.org/

- Ley orgánica 15/99 sobre la protección de datos de carácter personal. https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/Ley-15_99.pdf

- *Global voices en castellano* : http://es.globalvoicesonline.org/

- *Deeplinks Blog:* a cargo de la Electronic Frontier Foundation, informa puntualmente sobre derechos civiles y libertades en la red. Muchos de sus artículos son traducidos al castellano por su comunidad de voluntarios. https://www.eff.org/deeplinks

- Rebelión: Ha sido continúa en la actualidad como referente en castellano entre los medios contestatarios. Su apartado Conocimiento libre, agrupa publicaciones con licencia abierta de otros medios y colaboraciones directas de especial interés: http://www.rebelion.org/seccion.php?id=1

- *Wumingfundation*: Un grupo de escritores y creadores italianos que revolucionaron en su momento la creación en la red y explotaron nuevas formas de comunicación. En 2003 publicarían bajo el nombre colectivo de Luther Blisset el best seller "Q", una novela histórica. posteriormente cambiarían de nombre por el de Wu Ming (en alusión a un término chino que significa sin rostro) y publicarían otra novela titulada "54" con la que conseguirían un nuevo éxito. Todas sus obras son de código abierto y es precisamente el ser pioneros en este terreno lo que los señala de manera significativa. Su web actual: http://www.wumingfoundation.com/italiano/spanish_directo.htm#2003

- *Indymedia*: Una red de medios de información alternativos surgida en 1999 y que jugaría un papel muy importante en la creación de comunidades de activistas a través de la red. Su web: https://www.indymedia.org/es/

- *Nodo50*: El proveedor de servicios de Internet sin ánimo de lucro español que sería pionero en permitir que asociaciones y grupos de activistas pudieran tener voz en la red y gestionar servicios desde 1994. Sitio disponible en : http://info.nodo50.org/

Documentales

Como tantos otros recursos en Internet, los documentales promovidos por la comunidad son un elemento más de referencia. Entre los que proponemos aquí, están entrevistas directas a personas que han sido parte protagonista de varios momentos descritos en nuestra tesis. Lo más interesante de estos documentos audiovisuales es el valor de la entrevista directa con personas que forman parte de los temas que hemos descrito en nuestro trabajo.

- *Aaron Swartz. El Chico de internet. The Internet's Own Boy: The Story of Aaron Swartz*.: Sobre la historia de Aaron Stwartz Se produjo un documental financiado en la plataforma Kikstarter (https://www.kickstarter.com/projects/26788492/aaron-swartz-documentary-the-internets-own-boy-0) ,que finalmente sería subido a la plataforma YouTube https://www.youtube.com/watch?v=vXr-2hwTk58. También

cuenta con una reciente traducción al castellano en https://www.youtube.com/watch?v=czmVVU7uiBc.

- *TPB AFK: The Pirate Bay Away From Keyboard*: https://www.youtube.com/watch?v=eTOKXCEwo_8

- *CitizenFour.* El documental dirigido por Laura Poitras sobre el caso de Edward Snowden y las consecuencias de las revelaciones de este: https://citizenfourfilm.com/

- *Somos Legión La Historia de los Hactivistas*: https://www.youtube.com/watch?v=ee19z6D1yxo. Su web oficial: http://wearelegionthedocumentary.com/

- Canal de YouTube de OpenRightsGroup: https://www.youtube.com/channel/UCtZBMVI7r8HMHsTUkdrRABw

- *Amenaza Cyberhackers informáticos*. Del programa Informe Semanal, explica el caso de Estonia: https://www.youtube.com/watch?v=Z4X80QNOXc0

- Conferencia sobre Cibercrimen en Rusia*: Cómo y por qué actúan los ciberdelincuentes*, en el *I Qurtuba Security Congress:* https://www.youtube.com/watch?v=A0rySsa15nc

- *The hackers wars*. Un documental sobre los ataques de Anonymous y otros grupos : https://www.youtube.com/watch?t=221&v=YxFH4uJ9qXE

- *Everything is a remix*. Una serie de documentales que nos ponen en situación sobre la realidad de la creación original, la copia y el plagio. http://everythingisaremix.info/watch-the-series/

Asociaciones europeas de derecho digital:

- *EDRI*. Entidad de defensa de derecho digitales en Europa https://edri.org/
- *Open Rights Group*: OGN dedicada a la defensa de derechos digitales http://www.openrightsgroup.org/
- *Privacy Internacional*. Dedicada a temas relativos a la privacidad de las comunicaciones y la transparencia https://www.privacyinternational.org/
- *Panoptycon*: ONG griega de activismo en la red :http://panoptykon.org/
- *La Quadrature du Net*: ONG Europea, (francófona, a dedicada a la defensa de derechos y libertades en la red. Especialmente vigilante de las entidades europeas y sus acuerdos. http://www.laquadrature.net/
- *Free Software Foundation*: Especialmente enfocada en el Software libre y las libertades en la red. https://fsfe.org/fellowship/index.en.html

- *The Guardian Project* .Proyecto para salvaguardar nuestra privacidad mediante aplicaciones libres de espionaje, desarrollos Open Source https://guardianproject.info/

- *Xnet (exEXGAE*) La plataforma ciudadana de activistas frente al copyright y el abuso de los monopolios: https://xnet-x.net/

- La plataforma española de revelación y denuncia *Fítrala*, está destacando en las cuestiones de corrupción y las negociaciones secretas de tratados internacionales. Medios independientes españoles colaboran en el análisis y publicación de la documentación suministrada. Los medios son *Diagonal* (https://www.diagonalperiodico.net/), *El Diario* (http://www.eldiario.es).es, *La Marea* (http://www.lamarea.com) y *Mongolia* (http://www.revistamongolia.com/). La página del proyecto es : https://filtrala.org/

- *Caos Computer Club.* La mayor y más antigua asociación europea de hackers, especialmente alemanes. Especial relevancia los eventos anuales que suelen organizar: http://www.ccc.de/en/

- *Safe the Internet*. Iniciativa por la mayor parte de Asociaciones europeas en favor de la salvaguarda de la neutralidad de la red y la privacidad: http://www.savetheinternet.eu/

Asociaciones de activismo digital internacionales:

- *Electronic Frontier Foundation*: Una de las ONG más activas respecto a las libertades en la red y las legislaciones sobre el Copyright: www.eff.org

- *Access Now* es una de las organizaciones internacionales en favor de las libertades en la red que aglutina en sus campañas a otras organizaciones de ámbito nacional: https://www.accessnow.org/
- *Internet Society*: http://www.internetsociety.org
- *Freedom House*. Asociación dedicada a las libertades en diversos países. dispone de interesantes informes anuales sobre censura y libertades. Con especial mención a los medios y la red: https://freedomhouse.org
- *Citizen Lab* :http://www.citizenlab.org
- *Committee to Protect Bloggers* : http://www.committeetoprotectbloggers.org
- *Committee to Project Journalists* : https://www.cpj.org
- Berkman Center for Internet and Society: http://cyber.law.harvard.edu
- *FrontLine* https://www.frontlinedefenders.org
- *Global Internet Freedom* Consortium http://www.internetfreedom.org
- *The Herdict* https://www.herdict.org/web
- *Iniciativa OpenNet* http://opennet.ne
- *Peacefire* http://www.peacefire.org
- *Reporteros sin fronteras* http://www.rsf.org
- *Sesawe* https://sesawe.net
- *Tactical Tech Collective*: https://www.tacticaltech.org

- *Internet Defense League*:https://www.internetdefenseleague.org/

- Asociación internacional *Whisteblowing Press*. Una asociación que pretende garantizar la confidencialidad de las fuentes y la colaboración de medios independientes en su análisis y publicación. ,https://awp.is/

Algunas de mis colaboraciones periodísticas sobre temas tratados en esta tesis.

- *El avance de la Videovigilancia sin garantías ciudadanas*: http://www.rebelion.org/noticia.php?id=170707

- *Tu cara no es anónima* http://andradesfran.com/tu-cara-no-es-anonima

- *Big Data y la privacidad: Cuando el negocio eres tú*: http://www.eldiario.es/turing/BigData_0_120038458.html

- *Big Data. Cuando el interés comercial pasa por encima de la privacidad*: http://andradesfran.com/big-data-cuando-el-interes-comercial-pasa-por-encima-de-la-privacidad/

- *La guerra de los gigantes de internet y la prensa escrita*: http://andradesfran.com/la-guerra-de-los-gigantes-de-internet-la-prensa-escrita-y-el-viejo-conglomerado-mediatico/

- *Conexiones seguras, Privacidad y anonimato*: http://andradesfran.com/conexiones-seguras-privacidad-y-anonimato/

- *Las patentes como arma contra la competencia:* http://andradesfran.com/las-patentes-como-arma-contra-la-competencia/

- *El fin de la inocencia en la red* http://www.eldiario.es/turing/inocencia-red-internet_0_146635468.html y en http://www.rebelion.org/noticia.php?id=170310

- *TPP: Una negociación diseñada para favorecer intereses lobistas* : http://www.eldiario.es/turing/TPP-negociacion-favorecer-intereses-lobistas_0_137536755.html

- *Cinco escenarios de ciberguerra en el nuevo orden mundial:* http://andradesfran.com/cinco-escenarios-de-ciberguerra-en-el-nuevo-orden-mundial-actual/

- *Los dispositivos móviles y Android .Entre la libertad y el interés comercial* http://www.rebelion.org/noticia.php?id=170590

- *Sobre el escándalo PRISM, una de las primeras revelaciones de Edward Snowden*: http://andradesfran.com/prism-el-escandalo-de-espionaje-ciudadano-masivo/

- *¿Quién es Barrett Brown, el periodista especializado en espionaje que está en la cárcel?:* http://www.eldiario.es/turing/privatizacion-espionaje-periodista-Barret-Brown_0_150485289.html

- *¿Qué es el Hardware Libre?* :http://www.eldiario.es/turing/Hardware-Libre_0_139986451.html