INTERSTICIOS
Revista Sociológica de Pensamiento Crítico
ISSN 1887 – 3898

Vol. 6 (1) 2012

¿SEGURIDAD O CONTROL EN LA RED?: UN ANÁLISIS DEL EJERCICIO DEL PODER Y LA RESISTENCIA EN LOS ENTORNOS VIRTUALES A TRAVÉS DE LOS MEDIOS DE COMUNICACIÓN

Vanesa Bravo Nieto

Universidad Autónoma de Barcelona

RESUMEN

En una sociedad profundamente tecnológica, las actividades desarrolladas en los entornos virtuales forman parte de nuestra vida cotidiana entrelazándose hasta la indisolubilidad de la dicotomía real/virtual.

La información que se genera y mueve en estos entornos es difícil de calcular y aun más difícil de vislumbrar es a dónde y a quién va a parar dicha información. A raíz de esta dificultad surge el debate al respecto de la seguridad y los mecanismos de control en Internet, que a menudo entra en conflicto con el ejercicio de los derechos y libertades de sus usuarios.

La presente investigación trata de realizar un análisis del papel de los mecanismos de control y la resistencia al poder en los entornos virtuales, a través de su reflejo en los medios de comunicación.

Palabras clave: Biopoder, sociedad de control, medios de comunicación, hacker.

INTRODUCCIÓN

Los medios de comunicación se erigen como mecanismos de "reflejo" de la realidad en la que vivimos y tratan de exponer lo que en el mundo ocurre (Steven, 2005). Esta objetivación del relato de los fenómenos que acontecen genera un importante efecto en la población, ya que en parte sus opiniones, percepciones o ideas quedarán influidas y mediadas por lo que de ellos se desprenda.

La polémica al respecto del control/seguridad en Internet tiene también su lugar en los medios de comunicación. La expansión de las nuevas tecnologías y entre ellas como "buque insignia", Internet, ha abierto la veda

en los últimos años a la discusión al respecto de las acciones o actividades que en este marco pueden desarrollarse y los límites de las mismas.

A menudo, la información y el derecho a ésta se posiciona en el centro de la polémica, ¿debe controlarse el acceso a la información?, ¿es este control necesario para nuestra seguridad?, ¿quién debe tener el control de esta información? O lo que es más importante, ¿cómo se establece qué información debe ser protegida y cuál puede ser susceptible al acceso público?

El boom de las redes sociales o los blogs son algunos ejemplos que nos pueden ayudar a entender el volumen y circulación de información virtual que se produce hoy en día. Posteamos dónde estamos, con quién, qué hacemos, dónde compramos, qué nos gusta, qué pensamos y quiénes son nuestros amigos entre otras muchas cosas. Esta información queda al alcance de un gran número personas cuyos intereses pueden ser de variada índole y cariz moral.

Los mecanismos de control en este entorno planteados desde instituciones gubernamentales permiten mediante legislaciones y decretos establecer ciertos límites a las actividades y usos de la información que pueden o no realizarse. Por otra parte, los medios de comunicación tratan de dar un reflejo de las legislaciones estipuladas, las actividades y usos que la población ejerce fuera o dentro de esos límites y las repercusiones que la aplicación de la ley tiene sobre ésta. Finalmente, encontramos a los usuarios de dichas tecnologías que se encuentran en el centro de la polémica ya que por una parte, exigen cierta seguridad en su uso pero también se ven afectados por los mecanismos de control impuestos.

Estas interacciones pueden parecer a simple vista bastante sencillas pero las tecnologías de control, los mecanismos de poder (ya sean legislativos o de otro tipo), así como los medios de comunicación ejercen una notable influencia en los planteamientos, la ideología o la praxis de la población, y a su vez, debe tomarse en consideración los procesos de cuestionamiento o resistencia a este poder (Surman y Reilly, 2005).

En el tema que nos pertoca, podemos encontrar un “personaje” controvertido en lo que a prácticas en entornos virtuales compete. La figura del hacker ha sido tanto puesta en entredicho (Denning, 2001a, 2001b; Rodríguez, 2001; Trujano, Dorantes y Tovilla, 2009) como defendida (Aceros, 2006a, 2006b; Barandiaran, 2003; Jordan y Taylor, 2004; Roig, 2004; Samuel, 2001) dando paso a una amalgama de significados asociados que difícilmente nos ayuda a vislumbrar su papel en dicha controversia.

Por una parte, el hacker es considerado un entusiasta de la informática “motivado por el reto constante de conocer cómo funcionan las máquinas y los sistemas, de atravesar los límites que imponen las estructuras sistémicas, de (re)crear sistemas y de compartir esa creación, conocimiento y técnica con una comunidad que reconozca su valor”. (Barandiaran, 2003, p. 9)

Por otro lado, si atendemos a definiciones o posiciones planteadas desde medios de comunicación o a través de las especificaciones de las legislaciones vigentes sería un figura más cercana a la práctica delictiva. (Trujano, Dorantes y Tovilla, 2009)

Si tratamos de definir el debate, podemos atenernos a las dificultades para establecer esos límites entre la libertad, la posibilidad de acceso a la información, la protección de datos y el control. La barrera que separa el derecho a la privacidad y la violación de las libertades es a menudo difícil de definir. Los movimientos de resistencia y protesta ante los mecanismos de control presentes en la red aluden al uso lucrativo en beneficio propio de los datos recabados, la venta de informaciones privadas y al recorte de libertades y derechos en el uso en pos de la búsqueda de seguridad.

Los medios de comunicación alertan de actos delictivos cometidos en relación al robo y uso de informaciones y datos de carácter privado, la ruptura de sistemas de seguridad y daños en equipos o plataformas virtuales, a menudo asociados a estos mismos grupos de protesta.

Por su parte, las legislaciones tratan de establecer un rasero o medida de corte, que establezca los limites de las acciones permitidas o no en la red, pero por ello no quedan exentas de polémica ni parecen contentar a todos los actores de esta controversia ya sea alegando un excesivo recorte de libertades, o la ausencia de regulaciones precisas que reduzcan la inseguridad.

Las anteriores cuestiones permiten elaborar un primer esquema del estado de la cuestión ya que el tema es amplio y complejo. Por ello, para la profundización en el debate es necesario tratar cada uno de los ejes de la discusión por separado y en su interacción con los demás.

Se plantea un acercamiento a este debate desde el eje medios de comunicación-poder-grupos de resistencia, concretamente acercándose a las visiones que en la prensa escrita española se han arrojado al respecto del hacking (como estandarte de los grupos de resistencia en la red) y las cuestiones de seguridad y control en Internet.

La presente investigación se justifica en la necesidad de conocer los procesos, significados o acciones que sostienen el debate al respecto de la seguridad y control en la red.

El acercamiento a través de los medios de comunicación a lo que en cuanto a este debate se ha dicho permitiría establecer ciertas claves para su comprensión ya que es un debate central en los entornos virtuales durante los últimos años pero que nunca se ha tratado desde este punto de vista, tomando en especial consideración el papel que desarrolla la resistencia en este proceso.

MARCO TEÓRICO

Poder e influencia: El papel de los medios de comunicación en la conformación de subjetividades

> "Our societies continue to perform socially and politically by shifting the process of formation of the public mind for political institutions to the realm of communication, largely organized around the mass media." (Castells, 2007, p. 258)

Los medios de comunicación se han convertido a día de hoy en una poderosa fuente de información. El control que poseen sobre ésta -la información- que llega a nuestros hogares y la forma en que lo hace, media de manera fundamental en las opiniones de los espectadores/lectores/oyentes o simplemente sujetos pasivos ante la avalancha de mensajes, imágenes y sonidos que nos inundan a diario.

Los criterios de selección, así como su contenido valorativo implícito es otro de los aspectos fundamentales a destacar en la conformación del poder que los medios ejercen. Hardt y Negri (2000) afirman que:

> Ciertamente han existido previamente numerosos mecanismos para conformar la opinión pública y la percepción pública de la sociedad, pero los medios contemporáneos han suministrado instrumentos poderosos para estas tareas. Como dice Debord, en la sociedad del espectáculo sólo existe lo que aparece, y los medios principales mantienen algo cercano a un monopolio sobre lo que aparece ante la población. (p. 189)

En el análisis de dicha sociedad, el "espectáculo del miedo" (Hardt y Negri, 2000, p. 190) se constituye como la principal estrategia por la que los medios ejercen dicho poder sobre la población. Se alerta de los peligros, las sanciones y las dificultades, se regula el comportamiento de los sujetos a partir no ya del castigo directo

(el ejercicio de la disciplina) sino a través de la conformación de subjetividades bajo control, o más concretamente auto-control.

Los medios de comunicación no sólo nos informan, tratan de reflejar (con el consecuente sesgo) la realidad y en este proceso nos devuelve una mirada de nuestra sociedad que no sólo funciona como reflejo sino también como modelo que performa cómo debe ser.

> "Los medios de comunicación reflejan la dinámica del poder que actúa en cualquier sociedad, pero no simplemente reflejan, sino que proveen de símbolos, imágenes, ideas y marcos que constituyen el poder mismo." (Steven, 2005, p. 149)

El peso de las grandes corporaciones mediáticas que rigen el espacio informativo conforman a su vez centros de poder debido a su peso económico, y consecuentemente político (Lessig, 2004), a pesar de la existencia de los denominados medios de contra-información (Aceros, 2006a, 2006b; Castells, 2007; Steven, 2005) las escasas posibilidades y recursos de difusión de estos últimos los sitúan en clara desventaja.

Sin embargo, no es posible centrar el análisis de los mecanismos y formas de ejercicio del poder en los medios de comunicación. Éstos están influidos por otros medios y forman parte de la sociedad. Influyen en la sociedad, pero no debe olvidarse que están inscritos en dicho contexto, son a su vez influidos e influyentes, jugando un doble papel en las relaciones de poder existentes. (Steven, 2005)

Sociedad-red: La conformación de una sociedad profundamente tecnológica

> "El ciberespacio es la última forma de la cibernética social, es decir, de la interconexión de los individuos y de la puesta en red de lo viviente." (Mora, 2002, p. 2)

Las nuevas tecnologías atraviesan en la actualidad todos los aspectos de nuestra vida diaria. Las tecnologías y los entornos virtuales se interrelacionan de tal modo en lo cotidiano que los límites de división entre lo denominado "real" y "virtual" se evaporan hasta convertirse en un mero recuerdo.

Estas nuevas tecnologías nos han aportado facilidades en la realización de múltiples tareas y llevado a un nivel de comunicación y posibilidad de acceso a la información impensable hace sólo unos años. Nos "permiten transmitir, almacenar y conectar electrónicamente la información a través de diferentes espacios y tiempos. Su velocidad es enorme (y crece exponencialmente), su alcance planetario y su ámbito de acción casi universal" (Tirado, Rodríguez y Doménech, citados en Callén, 2006, p. 43)

Las distancias antaño difíciles de salvar y causantes del retardo de las informaciones son salvadas a día de hoy a golpe de click. La información se desplaza casi instantáneamente desde el momento de su producción; se transforma de un mero suceso local a la constitución de una red global de nodos interconectados. Las consecuencias de esta producción y distribución son obvias, tanto si atendemos al nivel más básico que sería la posibilidad de comunicación interpersonal como al nivel de estructuración social global e interconectada.

La "sociedad red" (Castells, 2001) en que vivimos está conformada por una estructura social "construida en torno a redes de información a partir de la tecnología de información microelectrónica, Internet, y otras tecnologías de biometría, telecomunicación y nanotecnología". (Callén, 2006, p. 43) Procesamos esta información y este nuevo plano de realidad para transformarlo en "nuestra" realidad, un todo integrado del que las tecnologías forman parte de manera indiscutible.

Sin embargo, "las máquinas y las tecnologías no son entidades neutras e independientes. Son herramientas biopolíticas desplegadas en regímenes específicos de producción que facilitan ciertas prácticas y prohiben

otras." (Hardt y Negri, 2000, p. 247) Constituyen un arma de doble filo, por un lado se convierten en condición de posibilidad de múltiples acciones, usos y ejercicios que de otro modo resultarían imposibles; pero, a su vez el control de dichas posibilidades (los límites de las acciones) constituyen un potente mecanismo de control social.

La estructura en red y la interconexión de los nodos por los cuales circula la información permite explicar el surgimiento de esta doble vertiente:

Por un lado, Internet (como estandarte de la sociedad-red) responde al modelo de rizoma de Deleuze y Guattari (1977). Se establece mediante una estructura de red desde la cual la información viaja a través de los diferentes nodos sin tener un punto central de partida y sin establecer distribuciones jerárquicas a priori. "(T)odos los nodos, independientemente de su localización territorial, se conectan con entre sí a través de una miríada de pasos y relevos". (Hardt y Negri, 2000, p. 176). Esta red aumenta las posibilidades de acción, establece una estructura desprovista a priori de desigualdades y en consecuencia, es el principal motivo que dificulta el control en estos entornos, ya que al no existir un punto central desde el cual se mueve la información, este control debería ser total e individualizado sobre cada uno de los nodos que establecen la red.

Sin embargo, si éste fuera el único modelo al que responde Internet, los problemas planteados al respecto de los mecanismos de control que recaen sobre la red y las limitaciones de las libertades y derechos en este entorno no existirían. El modelo oligopólico, se caracteriza por la conformación de un sistema de difusión de información y contenidos de manera unidireccional, un único elemento (o unos pocos) producen y difunden de manera centralizada las comunicaciones. Se establece como un modelo jerárquico de distribución masiva en que los puntos o nodos de recepción "son potencialmente infinitos y territorialmente indefinidos" (Hardt y Negri, 2000, p. 176).

Este modelo se corresponde con el seguido por las grandes corporaciones mediáticas, un número limitado de nodos difunden sobre la red sus comunicaciones de manera masiva y unidireccional.

Por tanto, la estructura de las comunicaciones y la difusión de la información se conforma de acuerdo a un híbrido entre ambos modelos. Su propia estructura permite cierta libertad y dificultad de control, pero, también facilita que las mayores posibilidades de difusión de la información recaiga en unos pocos nodos.

> La síntesis política del espacio social es fijada en el espacio de la información y la comunicación y sus tecnologías son herramientas biopolíticas, de producción de vida, desplegadas sobre regímenes específicos de producción que facilitan ciertas prácticas y dificultan otras. Se trata entonces de un nuevo plano para la acción y las experiencias que se entrelazan, hibridándolo, con nuestro mundo 'real'. (Callén, 2006, p. 44)

Biopoder

Después de las aproximaciones al entorno en el que se mueve la presente investigación, es necesario realizar un acercamiento más preciso a la concepción del poder con la que se está trabajando. Para ello, es indispensable partir de la conceptualización del poder -biopoder- en los trabajos de Michael Foucault.

Sus aportaciones en la comprensión del poder y las tecnologías de control serán fundamentales para establecer un paradigma desde el cual elaborar un acercamiento al debate en los entornos virtuales. A su vez, dicha noción será complementada por las concepciones de sociedad de control de Deleuze y los conceptos de extitución y biodatas, que nos aproximarán a una versión más actual de la concepción del poder adaptada al contexto de una sociedad profundamente tecnológica.

En el estudio del poder, ha existido una tradición tendente a realizar una "sociología jurídica del poder" (Foucault, 1976, p. 236) en el que éste es constituido desde las leyes y sus consecuentes prohibiciones. Es decir, se ha destacado el ejercicio de poder desde la vertiente jurídica que trata de enmarcar la localización del poder, desde dónde surge, quién lo ejerce y mediante qué reglas.

Foucault se desmarca de la tradicional concepción del poder en toda una serie de principios que se encuentran en su base: Por una parte, el poder es entendido como un ejercicio, es decir, no es algo que pueda pertenecer a alguien o que venga dado a determinada condición. El poder no se posee, se ejerce. No proviene de un lugar determinado sino que atraviesa toda la red de relaciones, y es la propia repetición de estas relaciones aquello que mantiene este poder, y a su vez, el poder deja de verse desde el punto de vista jurídico para ejercerse desde el punto de vista tecnológico.

Nada escapa al poder, todo está atravesado por él y las propias formas de resistencia no pueden sino surgir de los espacios de poder, desprendido de lo anterior, el poder necesita de la resistencia para su mantenimiento. (Hardt y Negri, 2000) La forma de articular esta resistencia según Foucault pasa por la necesidad de hacer evidentes los procesos de racionalización que se dan desde las estructuras de poder, no sólo en la crítica a la institución.

Es obvio que la existencia de legislaciones media poderosamente en el comportamiento de los individuos, pero es a menudo también el miedo a las repercusiones que el incumplimiento de las mismas producen, lo que constituye la base principal de la elección de las prácticas que se realizan. Se da una progresiva interiorización de la norma que deriva en la repetición de las prácticas de acuerdo a las regulaciones pero ya no por la influencia directa de las mismas sino por el control autoejercido por el individuo.

De la concepción del poder y su inscripción en los cuerpos se constituye la base del biopoder, siendo éste, "una forma de poder que regula la vida social desde su interior, siguiéndola, interpretándola, absorbiéndola y rearticulándola (…) el objetivo del poder es la producción y reproducción de la vida misma" (Hardt y Negri, 2000, p. 17).

Tecnologías de control

La caracterización del poder y su papel en la conformación de los sujetos está en estrecha relación con la noción de tecnologías, estableciendo cada una de ellas una forma de dominación.

Las tecnologías de poder, permiten el control externo del individuo a partir del ejercicio de poder normalizador, es decir, de la utilización de ciertos estándares a partir de los cuales la población queda impelida a mantenerse dentro de los márgenes estipulados de la "normalidad" a riesgo de padecer exclusiones derivadas de su incumplimiento.

Las tecnologías del yo, surgen de la interiorización de las normas anteriores; de este modo ya no es necesario que se ejerza control directo sobre la población ya que ésta lo ejerce sobre sí misma ante el temor por las represalias en el caso de conocerse la transgresión de la norma. De este modo el poder es sustentado por la construcción de subjetividades basadas en el propio control a tenor de las normas sociales, en este caso implícitas. El sujeto se autocontrola y se normaliza de acuerdo a los estándares sociales que ya forman parte de sus procesos de subjetivación.

Según Foucault (1990), "(c)ada una implica ciertas formas de aprendizaje y de modificación de los individuos, no sólo en el sentido más evidente de adquisición de ciertas habilidades, sino también en el sentido de adqui-

sición de ciertas actitudes". (p. 49) De este modo, de la unión o vinculación entre las tecnologías de poder y las tecnologías del yo surge la denominada "gubernamentalidad". (Foucault, 1978)

Como se apuntaba anteriormente, en la regulación de las prácticas y usos de la red en todos los ámbitos de nuestras vidas median los dos anteriores tipos de tecnologías mencionadas. Por un lado, se establecen regulaciones directas que marcan las líneas o los márgenes entre los cuales nuestras acciones pueden llevarse a cabo, y por otro lado, se establecen significados y asociaciones más profundos mediante su repetición que acabamos interiorizando y regulan nuestro proceder en el ciberespacio.

Se otorga al ejercicio de poder una noción de acción productiva, ya que permite crear objetos de saber y conocimiento. Surge la indisolubilidad del poder-saber que rompe en cierta medida con la tradición de la concepción del poder únicamente como acción de violencia.

La gubernamentalidad parte de la interrelación entre las tecnologías de poder y las tecnologías del yo. Ambas formas de ejercer el control, ya sea desde la exterioridad o desde la interioridad, quedan interconectadas y funcionan para el control de los sujetos en todos los ámbitos.

El análisis del poder bajo las sociedades de control: actualización de la concepción del poder en una sociedad tecnológica

Los trabajos de Deleuze permiten plantear el proceso de evolución desde la sociedad disciplinaria a la sociedad de control que establece un análisis más ajustado del poder en la sociedad actual.

Este autor, marca un importante cambio en la concepción del sujeto de poder. Si en las sociedades disciplinarias, el individuo era descrito por una marca y un número que lo posicionaba dentro de la masa, en las sociedades de control todo se reduce a un número que es usado a modo de contraseña, es decir, se conforma como la llave de acceso a la información, y el control de dicha información es fundamental para el ejercicio del poder.

> "Los individuos han devenido "dividuales" y las masas se han convertido en indicadores, datos, mercados o bancos". (Deleuze, 1995, p. 7)

Según Domènech y Tirado (2006), el "password" ha devenido la nueva llave del control. A partir de éste accedemos a múltiples extituciones[1], dejando tras nuestro paso toda una serie de datos, que entre otras cosas permiten la localización de nuestra trayectoria. De esta forma atraviesa las barreras físicas y temporales, dado que la información puede resultar accesible de manera continuada. Esta forma de control, a diferencia de la caracterizada por las instituciones, no es visible para el individuo dado que la base del control está en la posibilidad de movimiento y por ende, a mayor información disponible menor dificultad existirá en predecir la trayectoria de cada individuo.

La disciplina del cuerpo es sustituida por un control del movimiento y devenir a través de las posibilidades que brindan los dispositivos técnicos, de esta forma para la obtención de los datos es necesario establecer márgenes de libertad (libertad controlada por otra parte) a partir de los cuales el sujeto pueda generar movimiento para predecir trayectorias. Así, el acceso a la información se torna la principal herramienta de control de las nuevas anatomías de poder.

---

[1] Para la actualización de la noción de institución utilizada por Foucault es planteada la noción de extitución de Serres, (1994, citado por Domènech y Tirado, 2006). La extitución se constituye como la pervivencia de la vigilancia anclada en la posibilidad de movimiento.

Mecanismos de resistencia al poder en los entornos virtuales: el papel de los hackers en la protesta frente al control en la red

Al hablar de los mecanismos y grupos de resistencia al ejercicio del poder y las tecnologías del control dentro del ciberespacio, debemos tomar en especial consideración a los llamados hackers, o en su vertiente más política, hacktivistas.

Este trabajo se centra en los hackers o hacktivistas como ejemplo de la resistencia en los entornos virtuales por los siguientes motivos:

Por una parte, son los grupos o colectivos de resistencia en la red más conocidos por el público general, han sido protagonistas de numerosas noticias, libros o incluso películas. De acuerdo con esto, también su presencia en los medios de comunicación es más habitual; el hallazgo de referencias en torno a estos grupos es más numeroso y frecuente en los diferentes medios, convirtiéndose en estandarte de la lucha activa en la red frente a los mecanismos de control citados.

Si tratamos de definir de manera más precisa qué entendemos como hackers, ya se ha dicho que son personas entusiastas por el conocimiento de la tecnología que tratan de subvertir el funcionamiento convencional para generar nuevos usos y hacer avanzar estos dispositivos de acuerdo con las necesidades. Pero, a pesar de que puedan parecer desligadas del tema que nos concierne suelen ser prácticas con un fuerte contenido político.

> A pesar de que su práctica pueda ser apartidista (alejada de las instituciones ideológicas tradicionales) no puede dejar de ser micropolítica, no puede dejar de estar relacionada con la construcción tecnológica de las relaciones de poder que median la comunicación humana, que controlan los flujos de información, su manipulación y almacenamiento, que fijan posibilidades de intervención y de producción cognitiva (Barandiaran, 2003, p. 13).

Múltiples denominaciones (Campàs, 2003), que van desde hacktivistas (denominación empleada para hacer hincapié en el contenido político de sus acciones) o hackers, hasta crackers (se dice de la persona que rompe la seguridad de un sistema), lamers (aquellos que quieren realizar acciones propias de un hacker pero no poseen suficientes conocimientos técnicos para ello), phreackers (rompen la seguridad de los hilos telefónicos y hacen un uso ilegal de sus redes), o carders (aquellos que hacen un uso ilegal de tarjetas de crédito) juegan un papel clave en la constitución del fenómeno, ya que la diferenciación o la inclusión bajo una misma etiqueta de un conjunto variado de prácticas conlleva a su vez importantes implicaciones éticas y políticas. Estas prácticas pueden situarse en posiciones que van desde su inclusión en el denominado cibercrimen, ciberguerra, desobediencia civil electrónica, delitos virtuales, ciberprotestas o activismo político, siendo considerado movimiento social por algunos autores. (Aceros, 2006a, 2006b)

De este modo el planteamiento desde una u otra perspectiva conllevará a su vez una posición política con respecto al fenómeno. Aquella que asume dichos planteamientos como modo de acción política, tomará las prácticas y formas de hacer del colectivo como mecanismos de protesta legítimos para la consecución de los fines perseguidos. Sin embargo, desde la perspectiva que las acerca al terrorismo, dichas acciones serán plenamente deslegitimadas y constituirán actos delictivos que deberán ser perseguidos y sometidos a las correspondientes penas.

Por otra parte, y como ya se ha comentado anteriormente, estas prácticas se encuentran mediadas por las características del entorno en el que se mueven, en este caso Internet, pero también por la sociedad en la que se sitúan y sus características específicas. Chocan a menudo con discursos legales o discursos de los medios de comunicación que los enclavan en posiciones deslegitimadas de cara a la opinión pública a través

de su relación con el terrorismo o más concretamente cibercrimen. De este modo, sus actividades y principios están fuertemente atravesados por las influencias que estas perspectivas han tenido en los significados que les han sido asociados.

METODOLOGíA

El análisis de contenido como mecanismo de inferencia de significados

> "Qualitative research is a situated activity that locates the observer in the world. It consists of a set of interpretative, material practices that make the world visible. This practices transform the world." (Denzin y Lincoln, 2005, p. 3)

La metodología cualitativa permite el estudio de una gran variedad de materiales empíricos. La multiplicidad de sus métodos y técnicas permite tratar de dar sentido o realizar un acercamiento interpretativo al mundo y los fenómenos que en él ocurren en términos de los significados que la gente les otorga. (Denzin y Lincoln, 2005) Cada tipo de acercamiento posibilitará por tanto un tipo de entendimiento o interpretación de los fenómenos diferente.

De entre los métodos y técnicas que podemos incluir dentro de la metodología cualitativa, el análisis de contenido de los textos, permite no sólo abordar el contenido manifiesto de los textos o su forma, sino que permite extraer inferencias e indagar de manera más profunda los significados asociados de acuerdo al contexto en el que aparecen. Permite la interpretación de textos de diversa índole cuya característica común "es su capacidad para albergar un contenido que leído e interpretado adecuadamente nos abre las puertas al conocimiento de diversos aspectos y fenómenos de la vida social". (Abela, 2003, p. 2)

El análisis de contenido nos permite fundamentalmente realizar inferencias al respecto del material que estemos tratando, siempre tomando en consideración que "(l)os mensajes no tienen un único significado que necesite 'desplegarse'. Siempre será posible contemplar los datos desde múltiples perspectivas". (Krippendorf, 1990, p. 30) De este modo el papel de la persona investigadora deviene fundamental dado que sus decisiones e inferencias serán la base de las conclusiones y resultados de la investigación, como son la concreción de un marco teórico que dé sentido al análisis, la selección de las unidades de muestreo (en este caso, los fragmentos considerados más relevantes para los objetivos de investigación), el establecimiento de un sistema de codificación que permita trabajar con los fragmentos y el planteamiento de un sistema de control de la adecuación de dichos fragmentos para la investigación. (Abela, 2003)

Es obvio que la necesidad de acotar la información a analizar es fundamental para manejar un corpus de datos tratable, pero eso no implica que dichas decisiones sean tomadas a la ligera.

> Conviene no olvidar que determinar un sistema de categorías (categorizar) comporta realizar un juicio. Por ello, (...) es necesario que se definan con claridad criterios y pautas que especifiquen qué aspectos se han tomado en consideración al definir las categorías y cómo se ha hecho, así como también qué tipo de apreciaciones se han aplicado para decidir que una unidad de análisis debe formar parte de una categoría. (Vázquez, s.f., p. 9)

El producto final permite una articulación de los diversos fragmentos seleccionados de los textos para la creación de un nuevo texto en el que todas las informaciones, interpretaciones y relaciones de las mismas queden conformadas. No puede olvidarse que "(e)l propósito fundamental del análisis de contenido es realizar "inferencias". Inferencias que se refieren fundamentalmente a la comunicación simbólica o mensaje de los datos, que tratan en general, de fenómenos distintos de aquellos que son directamente observables." (Abela, 2003, p. 3)

La articulación de las informaciones viene anclada por las bases que comportan los objetivos de investigación y el marco teórico y conceptual empleado, que se convierte en el "cristal" o lente bajo el cual se miran y analizan los artículos y a su vez, un eje más de dicha articulación.

> Su propia denominación de análisis de "contenido", hace suponer que el "contenido" está encerrado, guardado -e incluso oculto- dentro de un "continente", se desvela su contenido (su significado, o su sentido), de forma que una nueva "interpretación" tomando en cuenta los datos del análisis, permitirá un diagnóstico, es decir un nuevo conocimiento (...) a través de su penetración individual. (Gaitán y Piñuel, 1998, p. 281)

Para el análisis de los textos periodísticos que hacen referencia al poder en los entornos virtuales y que permiten dar cuenta del contexto sociopolítico en el cual se inscribe el mismo, se han aplicado técnicas documentales cuyo objetivo es, según Íñiguez (1999), "la constitución de un corpus analizable en el marco de los distintos métodos" (p. 501), de esta forma este mismo autor describe el análisis de contenido y el análisis del discurso como los procedimientos más habituales.

Para ello, se ha realizado una selección y análisis de artículos de prensa escrita española de la última década a fin de tener una comprensión situada (espacial y temporalmente) y amplia de lo que en cuanto a control, poder y resistencia en los entornos virtuales (en especial aquellas informaciones que hacen referencia al hacking) se ha escrito en los últimos años.

La selección de los artículos y medios responde a la necesidad de acotar el volumen de información a niveles manejables. El periodo de publicación revisado se ha extendido desde enero de 2000 hasta marzo de 2010 en las ediciones impresa y digital de los periódicos españoles El Mundo y El País. Dichas elecciones no son arbitrarias: Los diarios de información general seleccionados cuentan con el mayor número de lectores (quedando excluidos los diarios de edición gratuita) y cuentan con hemerotecas virtuales que facilitan el acceso a ediciones y números anteriores. La selección de artículos aparecidos en prensa escrita permite mayor facilidad de acceso y análisis (tomando en consideración que abarcan un periodo extenso) y facilita a su vez tanto la existencia de un mayor volumen de material como una mayor extensión del mismo.

El hecho de remontarse hasta el año 2000 permite situarse en los años de mayor auge y expansión de Internet en cuanto a número de usuarios se refiere (entre los años 2000 y 2005 se registró en España un aumento del 170% en el número de usuarios según datos de Nielsen//NetRatings) y la evolución de los usos y prácticas en este medio, escenario a su vez de los mecanismos de control y prácticas de resistencia y protesta que nos interesan.

RESULTADOS

> "The relationship between technology, communication, and power reflects opposing values and interests, and engages a plurality of social actors in conflict" (Castells, 2007, p. 239)

Como ya se comentó anteriormente, las influencias entre los diferentes actores en el conflicto seguridad/control en la red, conforman una red de interacciones y significados cuyo análisis facilitaría la comprensión de sus papeles y conformaría un entendimiento aproximado del estado de la cuestión.

El papel de los medios es innegable en el asunto que nos compete. Del análisis de los 130 artículos de prensa seleccionados finalmente, se desprende una comprensión más cercana pero no por ello acabada de los actores clave en el debate.

Las principales conclusiones que pueden apuntarse son la identificación de algunas de las claves del conflicto y una conformación más precisa de lo que se entiende por resistencia al control en los medios.

La conformación del conflicto

> "La llamada sociedad de la información y el conocimiento no es pues un consenso, sino lugar de tensión entre las distintas fuerzas, vectores de territorialización y desterritorialización constante que se afanan por constituir el orden de lo social" (Callén, 2006, p. 41)

El papel de la prensa en el conflicto viene determinado por sus efectos e influencias hacia los sujetos. Lo que en la prensa aparece tiene importantes efectos sobre la opinión de los lectores. Por ello las informaciones y significados que transmiten son unas importantes fuentes de comunicación que llegan a la sociedad, de ciertos fenómenos. A partir de esto, es fundamental repasar las posiciones que surgen de los medios, al respecto de la polémica.

A su vez, es necesario tomar en consideración el papel de los proyectos de resistencia o denuncia a los excesos de control, ejemplificado en este caso en la figura de los hackers y su aparición en los medios de comunicación.

> "Both the powers that be and subjects of counter-power projects operate nowadays in a new technological framework; and this has consequences for the ways, means, and goals of their conflictive practice". (Castells, 2007, p. 239)

Ejercemos nuestras posibilidades de acción en la red, desempeñamos prácticas en entornos virtuales y estas prácticas son vistas desde puntos de vista contradictorios. Por un lado, tenemos el denominado derecho a la libertad de expresión, por otro lado, el derecho a la privacidad y si el asunto no resultaba lo suficientemente complicado, cerramos el triángulo con el derecho a la información. Tres derechos que conllevan igualmente múltiples obligaciones, tanto en su ejercicio como en la especificación de los límites que separan uno u otro.

En una entrevista realizada a Pekka Himanen se plantea que:

> "Hay dos grandes presiones sobre los hackers: las compañías que quieren tener información de nosotros y los gobiernos que introducen fuertes controles. Creen que cuanta menos libertad y privacidad, más seguridad; pero la historia de la Europa totalitaria demuestra que las sociedades son más inseguras cuando más limitada tienen la libertad" (El País, 21/3/2002)

Si concretamos más en los aspectos que mueven el debate encontramos por un lado, la controversia que provoca quién puede tener acceso a la información que generamos en la red. Facilitamos nuestros datos a empresas, instituciones, etc, y a su vez son enviados a otras de modo que informaciones referentes a nuestra vida se desplazan a gran velocidad para fines que ni siquiera conocemos, ya que habremos autorizado de antemano su uso, desde el desconocimiento.

Por otra parte, encontramos la problemática que se genera cuando estos datos, en principio protegidos por las empresas, quedan al descubierto debido a errores de seguridad. Podría darse el caso de que dicho fallo fuera detectado e informados los responsables de velar por su privacidad o en situaciones más adversas, que dicha información fuera utilizada en beneficio propio.

> "Según el comandante Juan Salom, responsable del Grupo de Delitos Telemáticos de la Guardia Civil, la intrusión en redes empresariales y el robo de datos confidenciales es uno de los crímenes de mayor impacto. El problema es que las empresas, por razones de imagen o seguridad, rara vez denuncian los hechos." (El Mundo, 18/7/2004)

> "Los ladrones de números de tarjetas de crédito se van a reunir en Odessa. El FBI ha detectado que las mafias del Este recurren a jóvenes informáticos para robar datos bancarios de los usuarios de comercio 'on line'. Sólo en Estados Unidos, se pierden 1000 millones de euros al año." (El Mundo, 30/5/2002)

Las dificultades para distinguir entre aquellos que persiguen uno u otro fin son las causantes de los significados contradictorios asociados al colectivo hacker que serán tratados más extensamente.

> "La imaginación, la curiosidad o la elegancia técnica son palabras clave de esta contracultura con mala fama, por los abusos que algunos han realizado enarbolando su bandera. Para contrarrestarlo, dan gran importancia a la llamada ética hacker, un código moral que incluye normas como no destruir redes ni ordenadores o respetar la libertad de información y la privacidad de los datos." (El País, 6/1/2007)

Una vez planteado el tema del acceso a la información encontramos el debate que generan los mecanismos de control que se utilizan en pos de dicha seguridad. Se revisan informaciones, se restringen ciertos tipos de comunicación y se persiguen ciertas prácticas. Estas estrategias son a menudo criticadas por su exceso de celo que roza la violación de libertades y derechos de los ciudadanos.

> "Aluden a que esta ley viola las libertades y derechos civiles de los ciudadanos y aumenta los controles para los usuarios de Internet." (El Mundo, 16/7/2002)

Aquí es donde entran en juego los procesos de resistencia y grupos de protesta cuyas prácticas se mueven en los límites entre lo prohibido y lo permitido, siendo perseguidos en numerosas ocasiones por presuntas vulneraciones de la ley.

Este se convierte en otro de los ejes del debate, ¿deben ser perseguidas estas acciones?, ¿son lícitas sus acciones? De la frontera entre delitos y prácticas aceptadas se hablará posteriormente.

Mecanismos de restricción y control

La legislación de los entornos virtuales, las medidas de seguridad cada vez más potentes de las empresas y las campañas mediáticas, parecen ser los mecanismos más frecuentes de control en estos contextos. "Sin duda nos enfrentamos a los intentos por parte de las grandes ISP de cercar Internet (Meikle, 2002 y Rheingold, 2003), al reforzamiento de las normativas regresivas sobre la propiedad intelectual y al surgimiento de los regímenes de vigilancia online (O'Siochru, 2003)". (Surman y Reilly, 2005, p. 6)

La estipulación de las prácticas y sus límites trata de ser una herramienta de demarcación del buen hacer en la red. Sin embargo, no sólo "castigos" y normas son utilizados en el ejercicio del poder. La conformación de subjetividades y la auto-aplicación de las normas suelen ser otras herramientas de potente utilización. Campañas mediáticas al respecto de la piratería informática que aluden a nuestro buen hacer, ética y sentido común conviven con otras que nos recuerdan los delitos y penas que conllevan las acciones que no nos están permitidas. Esta convivencia nos sirve como potente ejemplo de la pervivencia en una sociedad tecnológica de mecanismos de control propios de la sociedad disciplinaria (Foucault, 1976) y la sociedad de control (Deleuze, 1995).

A pesar de ello, las referencias más explicitas en la revisión de los artículos analizados a los mecanismos de control en la red son al respecto de legislaciones (ya sean vigentes o en proceso de aprobación):

> "El proyecto de reforma del Código Penal, recién llegado al Congreso para su debate, incluye en la exposición de motivos el término 'hacker' para explicar la posible ampliación del delito de revelación de secretos." (El Mundo, 22/1/2007)

> "El Congreso de Estados Unidos ha aprobado casi por unanimidad la Cyber Security Enhacement Act(CSEA), la ley que endurecerá y perseguirá sin trabas los crímenes 'electrónicos', y que permitirá que los 'hackers' más destructivos puedan ser condenados a cadena perpetua.[...] Son muchas las voces que se levantan contra esta ley, entre ellas, las de la Fundación para el Software Libre (Free Software Fundation) o la Asociación de Proveedores de Internet de Estados Unidos. Aluden a que esta ley viola las libertades y derechos civiles de los ciudadanos y aumenta los controles para los usuarios de Internet." (El Mundo, 16/7/2002)

Como puede observarse, las legislaciones forman parte de la polémica, el límite que marcan en las prácticas en la red es a menudo motivo de conflicto y protesta.

Procesos de resistencia al control en los entornos virtuales

> La máquina imperial es auto-validante, autopoyética – es decir, sistémica. Construye tramas sociales que evacuan o tornan ineficaces cualquier contradicción; crea situaciones en las cuales, antes de neutralizar coercitivamente lo diferente, parece absorberlo en un juego insignificante de equilibrio auto-generado y auto-regulado. (Hardt y Negri, 2000, p. 23)

La resistencia es inmanente a las relaciones de poder, trata de establecer resquicios de libertad que permitan el cambio en el ejercicio del poder a la vez que lo sustentan.

Las limitaciones y trabas que en el ejercicio del poder se imponen a los movimientos y acciones de protesta son múltiples. El análisis de los mensajes que desde los medios de comunicación se lanzan al respecto de las acciones políticas de rechazo puede permitir un acercamiento a los significados que se están generando de cara a la población. Por una parte, se ha afirmado que lo que no aparece en los medios no existe (Hardt y Negri, 2000) y por otro lado, lo que sí aparece es tremendamente influyente en los receptores de la información (Steven, 2005).

> "Los heterodoxos siempre han tenido mala prensa para quien ostenta el poder. El poderoso aspira al orden, y todo lo que no encaje en su esquema es considerado un peligro, una oportunidad para el caos. Y con ello el poderoso olvida que los sistemas rígidos acaban por anquilosarse, sólo lo flexible permanece". (El Mundo, 12/1/2008)

Hackers, hacktivistas y demás activistas tecnológicos son los ejemplo más conocidos de la resistencia al poder y control en los entornos tecnológicos. Su aparición en los medios no es masiva pero sí constante en la última década. Se configuran como figuras polémicas ya que no parece haber un consenso en el papel que juegan o en la legitimidad de sus acciones.

Mientras que en ciertos casos su figura es relacionada con actividades delictivas, en otros caso trata de separarse de dicha vinculación para categorizarlo como formas de acción política en la red.

> "Mitnick es el ejemplo clásico de la diferencia entre un hacker y un cracker. El primero, se entromete e incluso roba en los sistemas informáticos pero lo hace sin ánimo de lucro o de provocar daño. Por curiosidad intelectual o movido por la denuncia social. El cracker, igualmente habilidoso con la informática, es sencillamente un delincuente que busca su beneficio." (El País, 16/6/2006)

El intento de diferenciación entre hackers y crackers, es frecuente a lo largo de los artículos revisados:

> "A diferencia del cracker (rompedor), el hacker no es delictivo." (El País, 13/3/2003)

Sin embargo, no siempre es así, a menudo ambos términos aparecen entremezclados o empleados de modo indistinto dentro de un mismo artículo:

> "Se cree que los 'hackers' malintencionados o 'crackers', causan a los negocios mundiales pérdidas valoradas en miles de millones de dólares al año, y los costes por defenderse de ellos se están disparando." (El Mundo, 27/6/2004)

O en un artículo del 28/3/2009 de El País podemos leer en el titular: "Detenido un 'hacker' que acosa famosos", más adelante en el cuerpo de la noticia encontramos el siguiente fragmento: "El cracker (como se conoce al pirata informático que tiene fines delictivos)"

También encontramos la asociación de hackers y delitos de manera habitual en la prensa escrita, mediante el empleo de categorizaciones como "criminal" (El País, 25/6/2006), "Ya no hay ciberpunks, hay cibercrimen" (El País, 24/7/2008) o "delincuente informático." (El País, 28/8/2003).

Esta multitud de significados asociados (a la vez que contradictorios entre sí) es una importante razón que nos permite entender el porqué de la dificultad de comprensión que existe hacia la figura del hacker. Asociado comúnmente con delitos en la red, su papel en el conflicto a menudo es el de chivo expiatorio, se convierte en la denominación bajo la cual incluir todas las prácticas en la red que se encuentren en el limite de la legalidad o directamente incurran en delito. Sin embargo, esta cuestión no carece de implicaciones éticas y políticas.

A partir de su asociación con delitos en la red, es evidente que las acciones y propuestas desarrolladas por éstos comporten una total deslegitimación y no sólo esto sino que dichas actividades serán perseguidas y sometidas a sus correspondientes penas de acuerdo con las legislaciones vigentes. Así, podemos atender también a que estas acciones sean desprovistas de cualquier tipo de ética que incite a la acción y a su vez, carentes de contenido político (si esto es realmente posible).

Por otro lado, la adopción de la perspectiva desde la acción política o simplemente desde la curiosidad por el conocimiento de la tecnología y su mejora, conlleva una situación prácticamente opuesta a la anterior. Sus acciones no son vistas a priori como actividades ilegales y por tanto no serán perseguidas y reprendidas antes de su realización, es decir, se abre un curso de acción, una posibilidad para la resistencia. Es evidente que desde esta posición no se defiende la total impunidad de las acciones que puedan realizarse en nombre de este colectivo, pero sí al menos no están categorizadas de antemano como delitos, pudiendo apelar a una determinada ética que dirija sus acciones. No es una cuestión menor establecer un colectivo como grupo de resistencia a determinados entramados de poder o como agrupación delictiva. Los significados asociados, los posibles procesos de estigmatización e incluso los cursos de acción que se abren frente a ambos son lógica y totalmente diferentes.

El establecimiento de límites: la norma y el delito

> La síntesis política del espacio social es fijada en el espacio de la información y la comunicación y sus tecnologías son herramientas biopolíticas, de producción de vida, desplegadas sobre regímenes específicos de producción que facilitan ciertas prácticas y dificultan otras. Se trata entonces de un nuevo plano para la acción y las experiencias que se entrelazan, hibridándolo, con nuestro mundo "real". (Callén, 2006, p. 44)

La posibilidad de acción, de transitar y generar movimiento en la red es el elemento que facilita la generación de información, la herramienta del poder, sin embargo, el exceso de libertad en ese obrar o la apropiación de la información que es generada son otros de los aspectos sobre los cuales recae de nuevo el control.

El control de la información puede llegar a límites en los que la vida de una persona pueda estar en juego:

> "La información provenía de Roberta Gross, inspectora de la NASA, quien había revelado que un 'hacker' retrasó la transmisión de los latidos del corazón, pulso y otras condiciones médicas de los tripulantes cuando su nave se acoplaba a la estación espacial rusa Mir." (El País, 14/7/2000)

El límite que marca lo que es una actividad lícita y lo que debe quedar al margen de las prácticas permitidas es delgado y a menudo polémico. Ciertas acciones son permitidas o no según quién las lleve a cabo:

> "Berman anunció que presentará una ley que habilite a las compañías a lanzar ataques tecnológicos contra las redes de intercambio. 'La ley no permitirá la introducción de virus', aclara Berman, pero amparará otras tácticas ahora ilegales como la interdiction. Ésta consiste en hacer cientos de peticiones simultáneamente a un servidor y anularlas antes de recibir el archivo, bloqueando así el sistema." (El Mundo, 25/7/2002)

Es importante destacar el planteamiento constante de legislaciones al respecto de las prácticas y usos en la red. Su relativa novedad y la constante expansión de las posibilidades de dichos entornos genera una continua necesidad de renovación y adaptación.

Una de las formas de control más corrientes, consiste en la demarcación de las prácticas que pueden llevarse a cabo, sin embargo, esta limitación resulta un importante constreñimiento de las posibilidades y libertad de acción en la red.

Los mecanismos de protesta y resistencia suelen hacer uso de prácticas que se mueven en el límite de lo permitido, atravesándolo en ciertas ocasiones.

Esta transgresión de la norma, ha sido habitualmente relacionada con aquellos delitos virtuales que persiguen el beneficio personal de quienes la realizan, debido a la similitud en sus ejecuciones.

He aquí una de las problemáticas, la semejanza de sus acciones (a pesar de la diferencia en sus fines y objetivos) es una de las razones por las cuales hackers y hacktivistas son metidos dentro del mismo saco que meros delincuentes en la red.

> "Desafortunadamente, los medios parecen haber confundido los términos y fijarse solamente en el aspecto negativo de la ruptura de sistemas de seguridad." (El Mundo 2/11/2000)

La legislación y la norma suelen referirse a sus prácticas por lo que son investigados y los nuevos mecanismos de control tienden a perseguir las nuevas acciones y prácticas que desarrollan. Es decir, el entramado legislativo pone en marcha su maquinaria para inhibir las prácticas hacktvistas, antes de que éstas se produzcan; la ley surge a partir de las nuevas prácticas hacker como un intento para frenarlas y limitar las novedosas posibilidades de resistencia.

La delimitación entre simples usos de la red y delito son estrechas. Las tecnologías se convierten en condición de posibilidad de dichas prácticas pero también es fundamental tomar en consideración qué finalidades se persiguen a la hora de establecer dicho límite puesto que puede ser el elemento que decante hacia cierto lado de la balanza.

> "Los terroristas han mostrado un interés claro por las capacidades del 'hacking' y, o bien entrenarán a sus propios reclutas, o contratarán a otros de fuera con la vista puesta en combinar atentados físicos con 'ciberataques'". (El Mundo, 5/3/2010)

La información como eje clave

> "La creación, el tratamiento y la transmisión de información se convierten en las principales fuentes de productividad y poder" (Castells, 2001, citado en Callén, 2006, p. 41)

Sin la creación de datos a cuya propiedad y uso todos aspiran, el debate quizás carecería de sentido. La posibilidad de movimiento en los entornos virtuales no surge sólo como una nueva herramienta de acceso a información, sino también como espacio de generación de nueva información, ya sea esta de carácter público o la que venimos a considerar de carácter "privado". Privado porque suponemos que el ámbito en el cual dichas informaciones van a circular sólo es conocido por nosotros o aquellos que seleccionamos. Sin embargo, "(l)as empresas de medios de comunicación venden contenido, pero también venden a sus audiencias a los anunciantes. Para ambos propósitos, cuanto más sepan de las necesidades, deseos, gustos, (...) más fácil lo tendrán a la hora de venderles productos o venderlos a ellos como consumidores potenciales a los anunciantes". (Steven, 2005, p. 100-101)

Las informaciones que generamos permiten conocer en gran medida nuestros gustos, intereses, costumbres, ingresos, …, dicha información es de gran interés para múltiples actores sociales: Los gobiernos están interesados en nuestra tendencia de voto, las empresas en nuestros gustos y hábitos de consumo y los estafadores en la contraseña de nuestra tarjeta de crédito. Múltiples datos que circulan por la red a la espera de que alguien sepa descifrarlos son objeto de codicia por todos ellos. De este modo, el acceso a la información es la herramienta de poder más potente.

> "El hacker causó daños y reveló información personal, ya que se apropió de todas las contraseñas de acceso al servidor, poniendo en peligro el servicio de Internet". (El País, 27/1/2005)
>
> "El detenido es sospechoso de liderar una organización de hackers (piratas informáticos) que ha lanzado varios ataques informáticos contra entidades bancarias españolas para estafar a sus clientes, por medio de una técnica conocida como pishing". (El País, 30/7/2005).

El control ya no sobreviene por la limitación de las acciones sino por la percepción de libertad que tenemos, la libertad de movimiento. Sin embargo, es con este movimiento a partir del cual es posible trazar nuestros perfiles como votantes, compradores, usuarios, …, y actuar de acuerdo con ello.

CONCLUSIONES

Los mecanismos de control en la red son la base fundamental del debate sobre el poder en dichos entornos, cuyas posiciones extremas pasan por la búsqueda de la máxima seguridad a la denuncia de la vulneración de derechos y libertades de sus usuarios.

En el centro de dicha controversia se sitúa la información, cuyo acceso, posesión o control, sobreviene la base del poder. Transitamos por la red generando una amalgama de informaciones que permiten la generación de bases de datos más o menos precisas sobre nuestros gustos, intereses, preferencias de compra, opinión política, …, cuyo conocimiento facilita la manipulación y control.

Los mecanismos de control más directo (y también más nombrados de manera explícita en la prensa) son las legislaciones y normas que regulan los usos y prácticas en la red. Establecen los límites de nuestras actuaciones, y su infracción provoca un "castigo", una consecuencia negativa para quien lo realiza.

Los entornos virtuales constituyen ejemplo de la convivencia de la llamada sociedad disciplinaria (1976) con la sociedad de control (Deleuze, 1995). Marcamos los límites de nuestras acciones por miedo a las consecuencias que puedan tener pero no sólo; conformamos nuestros comportamientos y prácticas de acuerdo al

control (auto-control) que ejercemos desde nosotros mismos de acuerdo con la conformación de subjetividades.

Es de destacar el papel de los medios de comunicación en los procesos de conformación de dichas subjetividades. En su posición de comunicadores (más o menos fieles) de los fenómenos que acontecen y de la sociedad actual, no están ajenos al ejercicio del poder. Son influidos por la sociedad porque forman parte de ella pero a su vez, influyen en la sociedad revestidos de un poder "objetivador" de la realidad que transmiten. La influencia que ejercen en la percepción de los mecanismos de resistencia es fundamental.

En el caso que nos ocupa, la deslegitimación o la vinculación de grupos de protesta, hackers, hacktivistas, …, con la delincuencia en la red, tiene un potente efecto en los significados que les son asociados y en la posibilidad o margen de acción que se les confiere. De este modo, los medios de comunicación se convierten en actores clave en la controversia, ejerciendo y sustentando el poder.

> Los efectos: la creación de una esfera pública de consenso social aséptico y desprovеído de potencia política que facilite la subordinación de los productos de la multitud disidente bajo una única lógica comunicativa e informacional que se orienta a la supresión de las alternativas. (Callén, 2006, p. 57)

Para una mejor comprensión del debate entre seguridad/control y libertad, se hace necesario el análisis de las relaciones de poder existentes en el ciberespacio. Por una parte, como ya hemos dicho, la producción y control de la información recae sobre unos pocos nodos, que abogan por el discurso del control y la seguridad, deslegitimando a la otra parte litigante, los grupos de resistencia en la red, que enarbolan un discurso a favor de la libertad. El discurso normativo está respaldado por una serie de medios de comunicación de masas que ofrecen el reflejo de este posicionamiento al público general, provocando, mediante los mecanismos de control ya comentados, unos modos de actuar y un auto-control acorde a dicho discurso. Por ello, los requerimientos de una mayor seguridad en la red, así como un mayor control de lo que en ella ocurre y las acciones permitidas en los entornos virtuales, adquieren fuerza frente a la libertad de expresión/información, asociadas con unos grupos deslegitimados por los organismos y medios oficiales.

REFERENCIAS

Abela, J. (2003). *Las técnicas de análisis de contenido: Una revisión actualizada.* En: http://public.centrodeestudiosandaluces.es/pdfs/S200103.pdf Consultado el 29 de Diciembre de 2009.

Aceros, J. C. (2006a). *Ensamblar máquinas para construir sociedad*. Tesina presentada para el Doctorado en Psicología Social de la Universitat Autònoma de Barcelona.

Aceros, J.C. (2006b). *Jóvenes, hacktivismo y sociedad de la información*. Disponible en: http://www.sindominio.net/~txopi/Aceros_Jovenes_hacktivismo_y_sociedad_informacion.pdf

Barandiaran, X. (2003). *Hacklabs. tecnologías y redes de ensamblado colectivo de autonomía digital*. Disponible en: http://barandiaran.net/textos/hl/hl.pdf

Callén, B. (2006). *Tecnología... política hecha por otros medios. Una comprensión del tecnoactivismo desde Riereta.net*. Proyecto de investigación. Universidad Autónoma de Barcelona.

Callén, B. y Tirado, F. (2007). Biodatas y dividuos: La transformación de la biopolítica en la era de la información. En Tirado, F. y Domènech, M. (Eds.). *Lo social y lo virtual. Nuevas formas de control y transformación social.* Barcelona: Editorial UOC.

Campàs, J. (2003). *El paper d'Internet en la cultura emergent del món actual (1945-2003)*. Tesis doctoral en línea disponible en http://www.tdx.cat/TDX-0510105-120517

Castells, M. (2001). *Internet y la sociedad red*. Lección inaugural del programa de doctorado sobre la sociedad de la información y el conocimiento (UOC). Dsiponible en: http://tecnologiaedu.us.es/revistaslibros/castells.htm

Castells, M. (2007). Communication, power and counter-power in the network society. *International journal of communication, 1*, 238-266.

Deleuze, G. (1995). *Conversaciones 1972-1990*. Valencia: Pre-textos

Deleuze, G. y Guattari, F. (1977). *Rizoma: Introducción*. Valencia: Editorial Pre-textos.

Denning, D. (2001a). Activists and terrorists turn to cyberspace. *Harvard International Review, 23*(2), 70-75.

Denning, D. (2001b). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. *Networks and Netwars: The Future of Terror, Crime, and Militancy,* 239-288.

Denzin, N. K. y Lincoln, Y. S. (2000). *Handbook of qualitative research* (2nd ed.). Thousands Oaks, Calif.: Sage.

Domènech, M. y Tirado, F. (2006). Extituciones: Del poder y sus anatomías. *Política y sociedad, 36,* 183-196.

Foucault, M. (1976). *Historia de la sexualidad. vol. I: La voluntad de saber*. Madrid: Siglo XXI.

Foucault, M. (1976). *Estética, ética y hermeneútica*. Barcelona: Editorial Paidós Ibérica. (1999)

Foucault, M. (1978). La gubernamentalidad. *Tareas. Revista Del Centro De Estudios Latinoamericanos, 2000, 106*(6), 5-25.

Foucault, M. (1990). *Tecnologías del yo*. Barcelona: Editorial Paidós Ibérica.

Foucault, M. (1991). *Espacios de poder*. Madrid: Editorial La Piqueta.

Gaitán, J. A. y Piñuel, J. L. (1998). *Técnicas de investigación en comunicación social: elaboración y registro de datos.* Madrid: Síntesis.

Hardt, M. y Negri, A, (2002). *Imperio*. Barcelona: Editorial Paidós Ibérica.

Íñiguez, L. (1999). Investigación y evaluación cualitativa: bases teóricas y conceptuales. *Atención Primaria*, *23* (8), 496-502.

Jordan, T. y Taylor, P. A. (2004). *Hacktivism and cyberwars: Rebels with a cause?.* Routledge.

Krippendorf, K. (1990). *Metodología de análisis de contenido: Teoría y práctica*. Barcelona: Paidós

Lessig, L. (2004). *Por una cultura libre*. Disponible en: http://www.Elastico.net/archives/001222.html.

Mora, M. (2002). *Poder y resistencia en los entornos virtuales: notas sobre un debate sobre el fetichismo de las TIC y la desmovilización política.* Comunicación para el 1º Congreso online del Observatorio para la cibersociedad. Disponible en: http://www.edicionessimbioticas.info/Poder-y-resistencia-en-entornos.

Rodríguez, F.R. (2001). Hackers: El terrorismo virtual. *Revista de divulgación científica, tecnológica y cultural: Aleph Zero*, *23*, revista online disponible en: http://hosting.udlap.mx/profesores/miguela.mendez/alephzero/archivo/historico/az23/hackers.html

Roig, G.(2004). *Hackers: Activismo político en la frontera tecnológica.* Disponible en: http://consejoeps.uco.es/corsario/component/option,com_docman/task,doc_view/gid,16/Itemid,42/

Roig, G.(2007). Hacktivismo: Hackers y redes sociales. *Revista de estudios de juventud, 76,* 201-223.

Samuel, A. (2001). Decoding hacktivism: Purpose, method, and identity in a new social movement. *Harvard University. Unpublished Manuscript., 7*(31), Disponible en: http://www.Itas.Fzk.de/esociety/preprints/egovernance/samuel.pdf

Steven, P. (2005). *Dominatrix: La influencia de los medios de comunicación.* Barcelona: Intermón Oxfam.

Surman, M. y Reilly, K. (2005). Apropiarse de Internet para el cambio social. Hacia un uso estratégico de las nuevas tecnologías por las organizaciones transnacionales de la sociedad civil. *Cuadernos de Hegoa*, *38*.

Trujano, P., Dorantes, J. y Tovilla, V. (2009). Violencia en Internet: nuevas víctimas, nuevos retos. *Liberarbit, 15(*1), 7-19.

Vázquez, F. (s.f). *El dispositiu d'anàlisi de dades: l'Anàlisi de contingut temàtic/categorial.* Recuperado el 7 de Febrero de 2009 del sitio web del *Departamento de Psicología Social* de la Universidad Autónoma de Barcelona: http://psicologiasocial.uab.es/campus/mod/resource/view.phpinpopup=true&id=6507