# CIVILIZACIÓN HACKER

ALBERTO QUIAN

ANAYA MULTIMEDIA

# CONTENIDOS




# UNA REVELACIÓN HACKER

*«Sí, soy un delincuente. Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que vosotros, algo que nunca me perdonaréis».*

*—Loyd Blankenship, «The Mentor».*

Lo crea o no, Lady Gaga es hacker. Lo descubrí en diciembre de 2013, en una «revelación» de San iGNUcius, «patrón» protector de los hackers. «Lady Gaga es hacker de ropa», me dijo. Imaginé entonces a la diva del pop hackeando ropa inteligente, prendas que incorporan alta tecnología, como el sujetador con *bluetooth* True Love Tester (de la firma de lencería japonesa Ravijour), que mide el grado de excitación de una mujer mediante sus pulsaciones, de forma que, cuando alcanza un nivel máximo, una aplicación instalada en el teléfono móvil desbloquea el broche del sostén; o la prenda diseñada por Modesto Lomba en colaboración con la empresa de sistemas de climatización Baxi, que mide la temperatura corporal de quien la lleva puesta mediante sensores que envían una señal a una aplicación móvil que a su vez puede controlar el termostato del hogar, consiguiendo el ambiente perfecto; o la Trucker Jacket del proyecto Jacquard, de Levi's y Google, una chaqueta que permite utilizar un teléfono móvil inteligente sin sacarlo del bolsillo... Imaginé a Lady Gaga (premio Icono de la Moda del Consejo de Diseñadores de Estados Unidos por ser una «revolucionaria») sentada frente a un ordenador, programando compulsivamente, hackeando ropa inteligente... No había comprendido la «revelación» de San iGNUcius. «Nosotros, los hackers, aún insistimos en

su seguridad y privacidad están en manos negligentes, y nos advierten de que los sistemas deben ser mejorados para que no puedan infiltrarse en ellos auténticos delincuentes.

## HACKERS VS. CRACKERS

La criminalización de los hackers diseñada por el Estado-nación, diseminada por los medios de comunicación de masas e inoculada en la población se fundamenta en una arbitraria identificación de los miembros de esta comunidad como *crackers*, «los usuarios destructivos cuyo objetivo es crear virus e introducirse en otros sistemas», distingue Himanen.

A diferencia de los *crackers*, los hackers utilizan sus habilidades tecnológicas para resolver crisis en sus entornos por el bien común. Caballero y Cilleros aclaran en *El libro del hacker*: «Un hacker en origen no entra en sistemas ajenos con propósito malicioso o para beneficio personal», a diferencia de los *crackers*.

Según el *Jargon File*, el término «*cracker*» fue acuñado por los hackers en 1985 para defenderse del «mal uso periodístico» de la palabra «hacker». Su uso denotaba la repulsa de esta comunidad al robo y al vandalismo *cracker*. Esto no implica que los hackers se deban abstener de introducirse en sistemas sin permiso, pero siempre debe hacerse con un espíritu juguetón y curiosidad y por razones justificadas que no conlleven destrucción o daño alguno. Por ejemplo, se justifica que un hacker se adentre en un sistema informático ajeno para demostrar sus fallas de seguridad. Pero los esfuerzos de los hackers por desligarse de los *crackers* han sido tan intensos y constantes como infructuosos. La lucha contra el poder institucionalizado ha sido hasta ahora en vano. Los medios de comunicación dominantes mantienen la palabra «hacker» asociada casi exclusivamente a delitos informáticos, una práctica que hace comprensible el malestar que este uso perverso del término genera en la auténtica comunidad hacker, por suponer un ataque a sus valores implícitos.

La literatura hacker apenas ha alcanzado a la propia comunidad y a algunos investigadores y curiosos que han querido conocer las auténticas raíces de esta cultura, mientras una mayoría, «la masa», ha sido «infotoxicada» y empujada a la ignorancia por los aparatos dominantes de diseminación semántica del Estado-nación: prensa, radio, TV, diccionarios, informes institucionales y corporativos, etc., han impedido distinguir la ética hacker de la perversidad *cracker*. Raymond explica la diferencia ente los verdaderos hackers y los *crackers*:

> Los auténticos hackers [...] no quieren tener nada que ver con ellos [los *crackers*]. Los auténticos hackers piensan en su mayoría que los *crackers* son perezosos, irresponsables y no muy brillantes, y objetan que ser capaz de romper la seguridad [de un sistema] te convierta en un hacker [...]. La diferencia básica es esta: los hackers construyen cosas, los *crackers* las rompen.

Esta diferenciación entre hackers «auténticos» y *crackers* se origina en la propia comunidad hacker para contrarrestar el estereotipo negativo que han difundido los medios de masas. En este punto, es necesario recordar que el *hacking* no nace en la informática, ni se circunscribe, como ya hemos comentado, a la computación. El origen del uso de las palabras «*hack*» y «hacker» se halla en el Tech Model Railroad Club del MIT (creado en 1946), donde sus miembros empezaron, a finales de la década de 1950, a utilizar estos dos términos para referirse a sí mismos y sus técnicas. Fue en este club de modelos de trenes donde nació la cultura hacker. Y precisamente en la cuna del *hacking*, en su sitio web, el Tech Model Railroad Club dedica un apartado al *hacking*, donde se describe qué es ser hacker. Aquí, dejan también muy claro que hackear nada tiene que ver con delinquir:

> Aquí, en el Tech Model Railroad Club, donde se originaron las palabras «*hack*» y «hacker», y se han utilizado con orgullo desde finales de la década de 1950, nos molesta la mala aplicación del término para referirse a la comisión de actos ilegales. Las personas que hacen esas cosas se describen mejor con expresiones como «ladrones», «*crackers* de contraseñas» o «vándalos informáticos». Ciertamente, no son verdaderos hackers, ya que no comprenden la ética hacker.

Desafortunadamente para la comunidad hacker, muchos periodistas han sido engañados (o engañado) en el uso de la palabra «hacker» para describir lo que realmente hacen los *crackers* o cualquier tipo de ciberdelincuente; un engaño articulado por los aparatos de poder del Estado-nación y las grandes corporaciones tecnológicas, interesadas en criminalizar a una comunidad que cuestiona su hermetismo y un modelo comercial privativo y tirano que deja al consumidor en manos de la

de colaboración en red mediada por computadoras; la creación del ya mítico grupo hacker Legion of Doom, con miembros repartidos por Estados Unidos, y la aparición de la que es reconocida como primera organización hacktivista en el mundo, Cult of the Dead Cow, creada en Lubbock (Texas).

**Figura 1.4.** Macintosh 128K, el primer Mac de Apple, lanzado en 1984.

El 22 de enero de 1984, dos días antes de que Apple lanzase al mercado su primer Macintosh, millones de telespectadores fueron impactados durante la celebración de la Super Bowl (el mayor acontecimiento deportivo en Estados Unidos y uno de los más seguidos en el mundo) por un anuncio de la marca de la manzana mordida dirigido por el célebre director de cine Ridley Scott. No fue casualidad que Apple aguardase a que comenzara el año con el que Orwell tituló su sombría y distópica novela para iniciar la campaña publicitaria de su nuevo producto. IBM había sido tradicionalmente considerado el antagonista de la cultura hacker por quienes profesaban el *hacking* y Steve Jobs, ideólogo de Apple, se había curtido en la cultura hacker en sus primeros años, antes de pasarse al «lado oscuro» y traicionar los ideales de esta comunidad. Aquel *spot* aún hoy se considera uno de los mejores anuncios televisivos de la historia y permanece en la memoria colectiva de millones de personas. Los Macintosh venían para liberar al mundo del control de IBM, identificado por Jobs y los suyos como el auténtico Gran Hermano. En pleno fulgor hacker y efervescencia tecnológica, pocos podían imaginar que, tres décadas después, Apple y Steve Jobs serían vistos por los auténticos hackers como dignos herederos de IBM, como el Gran Hermano del siglo XXI, como un enemigo más de la libertad del individuo.

Veinticinco años después del estreno de este anuncio publicitario, Jon Lech Johansen (hacker noruego conocido por el alias DVD Jon, desarrollador del famoso programa DeCSS [Decoder Content Scramblins System]) realizó una adaptación de aquel anuncio en el que ahora es Apple quien representa al Partido, a la dictadura, y Steve Jobs es el Gran Hermano. Aunque no hay referencias explícitas a la marca ni a su fundador, el parecido del personaje de la pantalla (el gran dictador) con Steve Jobs es más que razonable, mientras la masa (seres anodinos) se muestra alienada por un aparato electrónico que simula ser un iPod, el producto con el que Apple inició una nueva era tecnológica. Jon Lech Johansen hizo este montaje para anunciar una nueva versión de la aplicación DoubleTwist, que, entre otras cosas, servía como puente entre iTunes y dispositivos que no son de Apple (un *hack* para saltar las barreras que Apple impone a sus consumidores con su sistema cerrado).

Nada parece fruto de la casualidad en la cultura hacker. En el año del Gran Hermano, Emmanuel Goldstein (enigmático personaje clave en la novela de Orwell, enemigo público número uno del Partido y amenaza para el Estado totalitario y su sistema de control y vigilancia) se encarnó en el editor de la nueva revista *2600: The Hacker Quaterly*. Esta publicación de culto entre la comunidad hacker no solo se convirtió en referencia contracultural, en mito del *underground* computacional, sino también en un ariete de lo que sería el hacktivismo. El sobrenombre fue tomado por el hacker y hacktivista Eric Gordon Corley para fundar en enero de 1984 esta revista, editada por su organización no lucrativa 2600 Enterprises, Inc.

1984 fue también el año de la «presentación oficial» de los hackers en sociedad, con la primera y gran apología de la cultura hacker, obra fundacional, fundamental y de culto: *Hackers: Heroes of the Computer Revolution*, de Steven Levy, elevó por primera vez a los hackers a categoría de clase social, y más concretamente, de élite en



# HACKTIVISMO

*«La verdad no conoce fronteras. La información necesita ser libre. La tecnología es la clave».*

*—Peter Gabriel.*

## DEL HACKERISMO AL HACKTIVISMO

Desde su misma germinación, en la cultura hacker se halla una inmanencia política que cuestiona el modelo y convenciones sociales, la organización del trabajo, la gestión estatal y corporativa de la información y los datos, y la privatización y comercialización del conocimiento. Sin embargo, esa inmanencia política ha trascendido y se ha manifestado en distintos grados y maneras en diferentes épocas y en distintas generaciones de hackers. Desde la aparente misantropía de las primeras generaciones de hackers, hasta la exhibición pública del gregarismo de las nuevas generaciones de hacktivistas, observamos que en sus acciones (ya sean solo para escribir nuevo software libre para beneficio de la comunidad o por pura diversión, o para introducirse en los sistemas de la autoridad para revelar sus secretos o cuestionar su seguridad) prevalece un espíritu libertario de defensa de la libre expresión e información y una apología de la voluntad y poder del individuo frente a la abúlica masa alienada. Sin embargo, ese espíritu libertario es por primera vez puesto al servicio de la defensa activa de los derechos humanos a partir de la segunda mitad de la década de 1990, cuando una vanguardia de hackers pasa

## INFOGUERRA DE BASE

La conceptualización de la «infoguerra» surge de la necesidad de elaborar una nueva doctrina militar ante las emergencias de un nuevo escenario geopolítico tras la caída del Muro de Berlín y del nuevo espacio «cíber» sin fronteras. Wray se remonta a principios de la década de 1990 para encontrar los orígenes de esta nueva doctrina militar. La caída del Telón de Acero, la disolución de la Unión Soviética y el consecuente ocaso de la retórica de la Guerra Fría como racionalización de la intervención extranjera; las nuevas guerras «inteligentes» y televisadas (seguidas por el gran público en tiempo real, como la de Irak) y el auge del ciberespacio hicieron que el aparato militar de Estados Unidos y sus centros de inteligencia, junto con sus aliados en sectores corporativos y financieros, viesen necesario elaborar una nueva doctrina militar. «Su respuesta fue la guerra de información y la amenaza "infoterrorista"», según Wray.

Este hacktivista describe lo que denomina «infoguerra de base» como una intensificación del activismo informatizado. Su aportación es el contrapunto al enfoque militarista de las «infoguerras». Para Wray, la distinción principal entre las formas anteriores de activismo informatizado y las formas de guerra informacional de base está en el grado de intensidad, el deseo de incitar a la acción y la capacidad para hacerlo a una escala global. Se trata de una guerra de palabras (una guerra de propaganda) que supone un primer paso para alejarse de la idea de Internet como simple espacio para la comunicación y el comienzo para transformar las palabras en hechos, en acciones directas. Más que un mero intercambio de información y de diálogo, lo que hay es un deseo de empujar las palabras a la acción, de usar medios alternativos en Internet como vehículos para incitar a la acción, en lugar de simplemente describir o informar.

Wray elucida que los actores de las «infoguerras» de base que emergen son plenamente conscientes de que están en un escenario global que les ofrece el don de la ubicuidad, capacidad de inmediatez y sentido de interconexión global.

A la clásica centralidad y jerarquía de la palabra dogmática del Estado-nación (*Dei Verbum*) se le opone ahora una nueva palabra performativa que surge del diálogo horizontal entre actores no estatales, que se distribuye por canales alternativos que compiten en el mismo espacio comunicativo (la Red) con los canales de información de la autoridad, que se confronta con el discurso oficial y lo desafía, que es generadora de ideas, argumentos y acciones, y que se configura como contrapoder.

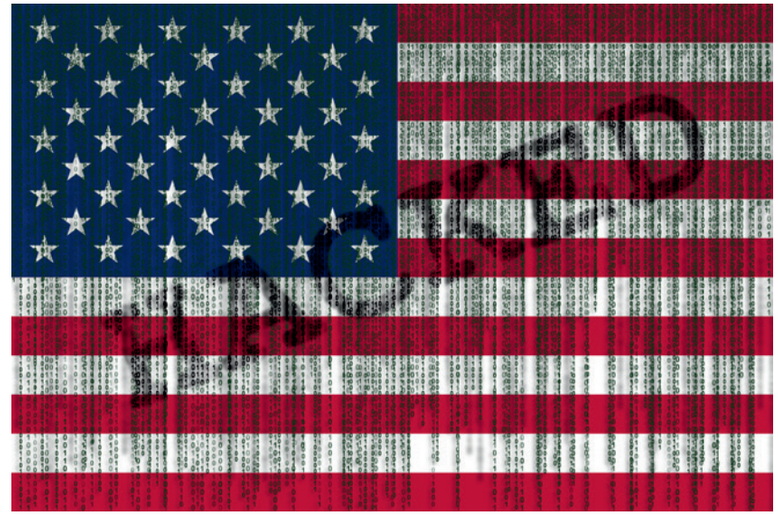

**Figura 2.2.** El Gobierno de Estados Unidos es uno de los principales objetivos de hacktivistas.

## DE LA DESOBEDIENCIA CIVIL ELECTRÓNICA A LA DESOBEDIENCIA CIVIL HÍBRIDA

La desobediencia civil electrónica es la tercera categoría en la que se manejan los movimientos civiles de resistencia en la Red. Es heredera de la desobediencia civil tradicional, descrita por Manion y Goodrum como una técnica de resistencia y protesta, cuyo propósito es lograr un cambio social o político dirigiendo la atención de la gente a determinados problemas e influyendo en la opinión pública. La desobediencia civil implica una ruptura pacífica de leyes que se consideran injustas; no tolera actos violentos o destructivos proyectados y sistematizados, y se centra en exponer injusticias y despertar conciencias. Es la misma visión aportada por el filósofo Ted Honderich en *Hierarchic democracy and the necessity of mass civil disobedience* (1995), donde describe la desobediencia civil como un llamamiento

zapatistas: el 10 de mayo, el 10 de junio, el 28 de junio, el 3 de julio y el 19 de julio. Pero fue el 9 de septiembre cuando el Electronic Disturbance Theater ejecutó la primera gran operación hacktivista de la historia.

La acción se desarrolló durante la celebración del Ars Electronica Festival,[16] en Liz, Austria, que aquel año se dedicó a las «infoguerras». La organización exhibió allí su proyecto SWARM (enjambre) y ejecutó un ataque masivo con FloodNet a tres bandas, dirigido contra un objetivo político, otro militar y un tercero económico: los sitios web de la Presidencia de México, el Pentágono y la Bolsa de Frankfurt. Con esta acción, los hacktivistas querían manifestar su apoyo a los zapatistas y su oposición al Gobierno mexicano, al Ejército de Estados Unidos y a la economía neoliberal global. FloodNet fue inutilizado en una acción a la contra del Departamento de Defensa estadounidense, que había diseñado un *applet* de Java hostil a FloodNet.

Unas veinte mil personas en todo el mundo se conectaron a FloodNet entre el 9 y el 10 de septiembre, pero sus golpes a los servidores no fueron suficientes para tumbarlos. El *applet* hostil generó serios problemas en los discos duros de los ciberactivistas e incluso obligó a muchos a reiniciar sus ordenadores. Al mismo tiempo, Wray (por entonces, doctorando) recibió un mensaje de correo electrónico de la Universidad de Nueva York en el que se le informaba de que la Agencia de Sistemas de Información para la Defensa de Estados Unidos se había quejado de contenido publicado por este estudiante sobre desobediencia civil electrónica, alojado en los servidores de la institución académica; finalmente, fue retirado.

La acción del Electronic Disturbance Theater resultó un fiasco técnico, pero fue una victoria simbólica, ya que primero resonó en los medios europeos, más tarde se hicieron eco de ella medios especializados estadounidenses como la revista *Wired*, el canal de televisión ZDTV o el periódico semanal *Defense News*, además de la red de estaciones National Public Radio, entre otros, y, finalmente, el hacktivismo saltó a la prensa generalista. Wray señala además la aparición aquel año de los primeros informes sobre hacktivismo en países como Reino Unido, Australia, India o China.

16. Ars Electronica, con sede en la ciudad austriaca de Linz, es una organización fundada en 1979 que premia cada año, desde 1987, los mejores y más vanguardistas proyectos de arte electrónico y digital de todo el mundo en siete categorías.



## EN EL FOCO DE LOS MEDIOS

1998 fue el año del salto del hacktivismo a los medios de comunicación de masas. El *Ottawa Citizen* fue uno de los primeros medios convencionales en ofrecer una descripción en profundidad de los hacktivistas. El 26 de octubre, el periodista Bob Paquin introdujo el término «hacktivista» en un amplio artículo publicado en este periódico con el título «E-Guerrillas in the mist». Paquin es uno de los primeros periodistas en describir al gran público el salto del *hacking* al hacktivismo, la materialización de código informático en acción política:

> Las primeras generaciones de hackers se deleitaban con el reto de explorar electrónicamente la geografía digital del nuevo paisaje que se creó a través de la revolución de la computadora. [...] Sin embargo, una segunda generación ha saltado a la palestra. Los llamados hacktivistas se dedican al ciberactivismo, o lo que algunos han llamado *hacking* ético.


**Figura 2.7.** La prensa ha dedicado innumerables titulares a hackers y hacktivistas.

En este artículo, el periodista describe algunas de las primeras acciones hacktivistas, entre las que recoge la del grupo mexicano X-Ploit, que en agosto de aquel año hackeó el sitio web del Ministerio de Finanzas de su país e incrustó

## TRES HÉROES DE LA LIBERTAD

### FILTRADORES: MANNING Y SNOWDEN

En WikiLeaks y en el nuevo hacktivismo es tan importante el código informático como el código emocional, con el que se apela a la conciencia de los individuos que trabajan en el centro neurálgico del poder para que filtren los secretos a los que tienen acceso como operarios del sistema.


**Figura 3.9.** Edward Snowden, en la prensa neerlandesa, tras revelar documentos secretos de la Agencia de Seguridad Nacional estadounidense (NSA) sobre su sistema global de vigilancia masiva, en 2013.

WikiLeaks ha inspirado a muchos potenciales filtradores a poner en el dominio público documentos de interés general que gobiernos y corporaciones ocultan a la ciudadanía. Y les ha asegurado, mediante tecnología de encriptación de información, la protección de su identidad. Ese fue el caso de la soldado Chelsea Manning, la exanalista militar que filtró en 2010 a WikiLeaks el vídeo de *Collateral Murder* y miles de documentos de las guerras de Irak y Afganistán y de cables diplomáticos de Estados Unidos. Que acabase siendo identificada, procesada y encarcelada no fue por un fallo en el proceso tecnológico de WikiLeaks, sino por un error humano de Manning.

En su libro *Dentro de WikiLeaks. Mi etapa en la web más peligrosa del mundo* (2011), Domscheit-Berg, excolaborador de Julian Assange, y muy crítico con este, defiende los procesos de esta organización para proteger a sus confidentes: «Nosotros no podíamos ni queríamos saber quiénes eran nuestras fuentes, eso formaba parte del concepto de seguridad [...] Su protección era nuestra mayor prioridad». De hecho, el sistema de comunicación encriptado era tan seguro que ni el propio Assange podía saber quién era la persona que le estaba enviando aquellos archivos confidenciales.

En el caso de Manning, lo que falló no fueron ni los protocolos ni los procesos tecnológicos de WikiLeaks, sino el factor humano. Manning había confesado a un exhacker, vía chat, que él era el responsable de las filtraciones a WikiLeaks de los documentos secretos de Estados Unidos. El exhacker en cuestión era Adrian Lamo, quien decidió delatar a Manning por filtrar 391.831 documentos de la guerra en Irak, 91.731 del conflicto bélico en Afganistán, 251.287 cables de la diplomacia de Estados Unidos, 779 documentos sobre presos en la base militar de Guantánamo y el dramático vídeo de *Collateral Murder*, grabado el 12 de julio de 2007 desde un helicóptero Apache estadounidense en Irak, en el que se ve cómo soldados estadounidenses acribillan al reportero de la agencia de noticias Reuters Namir Noor-Eldeen, a su ayudante y a diez civiles más.

Lamo justificó su denuncia alegando que aquellas filtraciones ponían en riesgo vidas. Sin embargo, jamás hubo evidencias de que hubiese muerto alguien como resultado de la información filtrada.

¿Por qué Manning le confesó su secreto? Lamo se había ganado la confianza de Manning (por entonces su identidad de género era masculina), quien le admiraba por haber sido un hacker famoso que ya había tenido encontronazos con el FBI y la justicia por sus actividades informáticas, especialmente por haber penetrado en la red informática de *The New York Times*, modificar sus bases de datos y añadir su nombre a la lista de columnistas del periódico. Por lo tanto, Manning fue




# APRENDIZAJE HACKER

*«La información es poder.*
*Pero, como todo poder, hay quienes se lo quieren quedar solo para ellos».*

*—Aaron Swartz.*

Hablar de hackers y hacktivistas a audiencias manipuladas por las falacias políticas y corporativas, y por el sensacionalismo periodístico, no es fácil, ya que el prejuicio ha sido inoculado a las masas durante décadas, desde los años ochenta del pasado siglo, para estigmatizar y criminalizar un movimiento contracultural con una ética basada en el trabajo libre y colaborativo, el saber compartido, la libertad de expresión, la libre información, la transparencia, el bien común y la defensa de los derechos humanos, incluidos los derechos a la privacidad y a saber mediante el libre y universal acceso a todas las fuentes de conocimiento. Gobiernos, empresas y medios han hecho pensar a las masas que ser hacker es sinónimo de delincuente informático y que el hacktivismo (la expresión política del *hacking*) es un «ismo» terrorista.

Es obvio que hackers y hacktivistas incordian a la autoridad. De ahí el relato criminalizador sobre ellos, aceptado como dogma de fe en los medios de masas tradicionales.

Cuando lea un titular en prensa en el que se usen las palabras «hacker» y «hacktivista» para referirse a delincuentes informáticos, cuando vea que un medio identifica un robo o una estafa con un hackeo, recuerde, le están mintiendo. Porque los hackers, los auténticos, no buscan causar daño, sino explorar los límites de lo

Si quiere conocer la historia de nuestra civilización digital, debe conocer la historia de los *hackers*. Mancillados por muchos, idolatrados por menos, los *hackers* han contribuido de manera decisiva al desarrollo de algunos de los más importantes artefactos e ingenios intelectuales de la revolución digital, empezando por la Red o el nacimiento de Apple.

Los inicios de la historia de la cultura y ética *hackers* se remontan seis décadas atrás, cuando jóvenes entusiastas y bromistas del Tech Model Railroad Club del MIT autodefinieron sus prácticas como *hacking* y a ellos mismos, como *hackers*. Este libro traza, desde entonces, la línea evolutiva de la cultura y ética *hackers*, con la cual se explica cómo y por qué han surgido en los últimos años fenómenos como WikiLeaks o los Anonymous, el auge de la criptografía o movimientos por el software libre y el reconocimiento del acceso abierto al conocimiento como derecho humano.

Este libro compone un complejo puzle mediante un análisis teórico, conceptual, histórico, interpretativo y crítico de la ética y la cultura *hackers*, y del hacktivismo como manifestación política del *hacking*. Recorriendo la historia de la comunidad *hacker*, con sus fuentes primigenias, conocerá los pilares de una nueva civilización.

ANAYA MULTIMEDIA
www.anayamultimedia.es

ISBN 978-84-415-4534-2
2315173