CiberÉtica como ética aplicada: una introducción

Javier Romero Muñoz
Facultad de Filosofía,
Universidad de Salamanca
jromero@usal.es

CyberEthics as Applied Ethics: an Introduction

Resumen: La ética aplicada surge en la relación de las distintas esferas sociales con los problemas morales y éticos. Un tema reciente en las discusiones y debates ha sido el avance tecnológico-informático, en el que se entrelazan la informática, la ética y la información. Como ética aplicada surge la CiberÉtica, un espacio nuevo de conocimiento y reflexión entre la informática y la ética.
Para orientar nuestro objetivo de introducción, habremos de ofrecer tres aspectos sobre el asunto: 1) analizar la sociedad en la era de la información, 2) relacionar el análisis con la CiberÉtica, y 3) mostrar las áreas y subáreas de la CiberÉtica. Finalmente, la ética hacker posee seis principios que la comunidad de hackers incorporan en su vida y trabajo técnico desde 1980.

Palabras clave: CiberÉtica, Ética Aplicada, Hackers, Ética dialógica, Ordenadores

Abstract: Applied Ethics arises in the relationship of different social areas with the ethical and moral problems. A recent topic in these debate has been the technological and computer advancement, in which computer, ethics and the information intertwine. As applied ethics CypherEthics arises, a new place of knowledge and thought between computer science and ethics.
To guide our introduction objective, this paper offers three aspects about this issue: an analysis of society in information age (1), an analysis of the relationship between information age and CyberEthics (2), and an evidence areas and subareas in CyberEthics (3). Finally, the Hacker Ethic has six principles that communities of hackers embody in their life and technical work since 1980.

Keywords: CyberEthics, Applied Ethics, Hackers, Dialogical Ethics, Computers

ISSN 1989-7022

A los miembros y amigos del Instituto Nacional de Ciberseguridad (INCIBE)

1. Introducción: El paradigma digital en la *era de la información*

El desarrollo de las relaciones económicas, políticas, sociales y culturales sobre una naturaleza que les sirve de base o de infraestructura, ha adquirido en las últimas décadas una dimensión particular. Conceptualmente esta nueva dimensión ha sido caracterizada como *globalización*, muy ligada a la economía de *laissez faire* como globalización de mercados financieros y de mercado internacional. Más allá de la unívoca visión económica, la globalización presenta multitud de predicados para su análisis: globalización ambiental, globalización cultural, globalización política, globalización económica, globalización de las comunicaciones, globalización de los derechos humanos y globalización de los riesgos e inseguridades. Esta nueva era, caracterizada por el sociólogo Manuel Castells como *era de la información*,

Received: 25/04/2017
Accepted: 03/05/2017

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

presenta un nuevo paradigma en el ámbito económico, sociológico, cultural, tecnológico, político y ecológico post-1989. Este nuevo paradigma podría clasificarse en cinco procesos:

1. La flexibilización de la economía de la gestión junto con la globalización del capital, la producción y el comercio,
2. Las exigencias de unos valores de libertad, democracia, privacidad y flujos de comunicación abierta de una sociedad civil en auge,
3. Los grandes avances tecnológicos en informática y telecomunicaciones debidos enteramente a la revolución dada en microelectrónica en su aplicación empírica de la mecánica cuántica y la teoría de la relatividad general,
4. La interdependencia entre los diferentes Estados nacionales en un marco transnacional de gobernanza global,
5. La ecodependencia planetaria entre los diferentes biomas naturales, junto con la atmósfera y las sociedades humanas y no-humanas.

Estos cinco procesos muestran una realidad global entretejida por encima de las fronteras territoriales y nacionales, donde el "efecto mariposa" de la *teoría del caos*, esto es, cómo el aleteo de una mariposa en el Amazonas podría desencadenar un huracán en otro lado del planeta[1], opera en numeras áreas ecológicas, culturales, tecnológicas, políticas y económicas. Uno de los hechos más significativos en los albores del siglo XXI ha sido el surgimiento de un Internet global, que se encontraba primeramente aislado en una pequeña comunidad científica de ingenieros informáticos, *hackers*, posibilitando una nueva realidad social, la *sociedad red* (Castells, 1998, 76-78). Si bien puede caracterizarse la invención de la rueda o la imprenta como inventos tecnológicos fundamentales en la Historia de la humanidad, Internet y las nuevas tecnologías de la información representan un paradigma único en el tiempo que entrópicamente está cambiando nuestras vidas.

El nacimiento de Internet puede dividirse en dos etapas: la etapa pre-1970 y la etapa post-1970:

> Etapa pre-1970: *Esta primera etapa correspondería a la creación de la red de ordenadores ARPANET por el Departamento de Defensa de Estados Unidos (ARPA), con un mapa lógico que llegó a conectar incluso sesenta ordenadores. A esta red de telecomunicaciones sólo tenían acceso un determinado grupo de militares y agencias de inteligencia (recordar al respecto que la CIA y la NSA fueron creadas paralelamente después de la segunda guerra mundial), con la finalidad, en plena* guerra fría*, de llevar a cabo una transferencia de datos a larga distancia*

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

y en poco tiempo mediante paquetes *de información (packets). El secretismo y opacidad de ARPANET por el Gobierno americano, llevó a una segunda etapa post-1970 en el nacimiento de Internet.*

Etapa post-1970: *Esta segunda etapa se caracterizó por el intento de llevar a las Universidades y a la sociedad civil los grandes avances dados en telecomunicaciones. La imposibilidad de acceso al proyecto militar llevó a los ingenieros de la Universidad de Illinois a establecer centros de supercomputación (TCP/IP)*[2]*, que facilitasen el acceso y la comunicación pública entre usuarios de la Universidad a 56 Kb. (person-to-person network). Estos avances fueron respaldados y ampliados por la Universidad de Michigan (NSFNet), llevando su desarrollo a la creación de la primera página web por Paul Kunz en 1991 (Stanford Linear Accellerator, SLAC). El protocolo* http *(hyper text transfer protocol) supuso una explosiva revolución tecnológica en el campo de los buscadores web: Mosaic, Netscape, Mozilla, Firefox, Internet Explorer, Yahoo! o Google, aumentando su seguridad con el protocolo* https *en la aplicación de los sistemas de cifrado asimétrico RSA para sistemas de cifrado clásico y no cuántico (presente en páginas de correo electrónico, redes sociales, cuentas de banco online, compras online, administraciones públicas, firmas electrónicas o digitales, etc.). Con la creación de diferentes buscadores y el impulso de las empresas de telecomunicaciones, la globalización de Internet expande sus raíces por todo el mundo. El desarrollo de diferentes páginas web de información, conocimiento, comunicación, periodismo, compra, etc., han estado en constante crecimiento hasta la actual interconexión total desde diferentes dispositivos. Esta interconexión se ha incrementado en los últimos años debido al Internet of Things (IoT), y a la posibilidad de una ciudad interconectada como hito futuro (smartcity), según los últimos avances presentados por las grandes empresas tecnológicas (como Google, Facebook, Microsoft, Apple, Intel o empresas de telecomunicaciones), o en los análisis llevados a cabo en los foros de hackers más importantes del planeta, como la DEFCON en Las Vegas, Black Hat en EEUU y Europa, o la Chaos Computer Club en Berlín.*

Con la evolución de los sistemas de comunicaciones y los protocolos base, Internet puede considerarse a día de hoy como una tecnología presente en muchos aspectos de la vida humana: laborales, científicos, económicos, emocionales, familiares, políticos, artísticos… Los datos empíricos publicados a finales del 2015 por *Internet World Stats*, afirman que alrededor de 3.366 millones de usuarios, un 46.4% de la población mundial, usan dicha tecnología para realizar todo tipo de operaciones profesionales y personales en diversos ámbitos y desde diferentes dispositivos con conexión red[3]. Paralelamente al desarrollo de la visión de una red de comunicaciones "perfecta" mediante un Internet global dominado por una sociedad anclada en la *tecnofilia*, se ha desarrollado un debate ético y político –presente en los foros internos de seguridad informática- sobre el uso y abuso de la nueva *red de redes*: libertad del usuario de acceso total a su computadora mediante la liberación del

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 45-63

código fuente, *software libre*, *hardware libre*, técnicas *hacking* de metasploit o test de penetración en sistemas, flujo de información abierta en los diferentes rastreos de IP o en los metadatos ocultos que genera un usuario en documentos ofimáticos, fotografías o impresoras, libertad de expresión en la red, privacidad absoluta de navegación, correos cifrados para una comunicación sin intermediarios, modelos neo-tecnocráticos de dominio y control de multinacionales de la informática y agencias de inteligencia, acción ciberpolítica, moneda digital *Bitcoin*, *Big Data*, cibercrimen, etc. Todos estos factores, que no han sido analizados correctamente por la filosofía actual, aún siendo un acontecimiento relevante para la humanidad, se presentan a día de hoy sintetizados dentro de la ética aplicada como CiberÉtica, un nuevo campo entre la ética y la informática[4].

El siguiente artículo busca introducir al lector, de un modo sintético y claro que sirva para posteriores análisis, publicaciones, conferencias (EthicsCON), comités, trabajo empírico en sistemas institucionales públicos o empresas particulares, a una nueva línea de reflexión práctica sobre los diferentes problemas morales que se identifican en la *sociedad red*. Para ello se presentará en primer lugar una introducción a qué es la CiberÉtica en el contexto del *giro aplicado* dado en filosofía moral y política (2), observando la necesaria clasificación en áreas y subáreas de los diferentes campos de análisis (3), para finalmente introducir y aclarar al lector sobre el uso del término *hacker* en este artículo, observando la ética interna que está detrás de su filosofía (4). A ello hay que sumar la bibliografía utilizada y una serie de páginas web sobre diferentes órganos institucionales públicos españoles relacionados con la práctica CiberÉtica.

2. La CiberÉtica como ética aplicada entre la ética y la informática

En las sociedades moralmente pluralistas y democráticas, *la* ética no existe, existen en verdad diversas morales en el ámbito cotidiano (morales religiosas o determinados proyectos personales de *vida buena*) y distintas líneas desde la filosofía moral (utilitarismo, kantismo, personalismo, eudemonismo, hedonismo, pragmatismo, etc.). Ninguna de ellas es hegemónica para toda la humanidad, ninguna de ellas es *la* moral o *la* ética. Es en este *politeísmo de los valores* –Weber *dixit*- donde el único camino posible es una teoría moral dirigida a la universalidad de los intereses y a la justicia (social, ambiental y comunicativa). No es caso paradójico observar cómo las

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

teorías contemporáneas de base racional –como paralelamente encontramos en J. Rawls y J. Habermas- esencialmente se formulan como teorías de la justicia con una fuerte impronta universalista. En el caso de Habermas, la finalidad de su proyecto ético-moral consistiría en *fundamentar* el "principio de universalidad" (U), que permitirá dar validez a nuestros enunciados y principios morales en una sociedad plural (más allá de la posición estática de J. Rawls). Para nutrir de información, reflexión y orientación a una forma nueva de deliberar los problemas morales con la finalidad de proponer recomendaciones para la acción, hay que hablar en primer lugar del estatuto característico que ocupan las éticas aplicadas (2.1), para analizar cómo la CiberÉtica, como ética aplicada, podría encuadrase en esta tradición (2.2).

2.1. El estatuto de las éticas aplicadas: diálogo intersubjetivo y consenso

La ética aplicada, o mejor dicho, las éticas aplicadas, poseen un lugar característico y reconocido en las sociedades pluralistas del siglo XXI. El punto de partida es observar que *la razón práctica*, que orienta la acción humana o a la forma de obrar en el mundo, puede dividirse en la actualidad en: (a) razón práctica de *uso pragmático* (razón instrumental orientada a fines), (b) razón práctica de *uso ético* (proyecto de vida personal), y (c) razón práctica de *uso moral* (justicia intersubjetiva) (Habermas, 2000, 109-126). En relación con este último *uso* se forman las éticas aplicadas como nuevo campo de estudio para la filosofía práctica en las sociedades pluralistas (¿qué debo/debemos hacer?). Su nacimiento en la década de los años sesenta y setenta del siglo pasado, se debe al intento de redefinir los principios y la metodología adecuada para analizar los diferentes dilemas ético-morales que plantean numerosas áreas de la realidad social, sobre todo en relación con el avance tecnológico de las últimas décadas. Su finalidad sería ofrecer respuestas adecuadas pensadas interdisciplinariamente desde la ética o filosofía moral, como campo de reflexión del obrar humano, en respuesta al "pluralismo ético" presente en las sociedades postmetafísicas. La importancia de las éticas aplicadas y su contribución a la sociedad ha sido tan característica y relevante en los últimos años, que puede hablarse a día de hoy de "giro aplicado" de igual manera que se habla de "giro lingüístico-hermenéutico" (R. Rorty y J. Habermas), "giro pragmático" (R. Bernstein), "giro deliberativo" (J. Dryzek) o "giro dialógico" (S. Rahman). Algunas ramas de aplicación en ética aplicada serían: la bioética, la ecoética, la ética económica y empresarial, la ética de los medios de comunicación, la neuroética, la ética profesional, la ética del deporte, etc.

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 45-63

Este tipo de *saber* es todo menos estático, es decir, no es definitivo y está en constante construcción intersubjetiva y dialógica entre todos los sujetos que participan del dialogo (de ahí que se requiera un aprendizaje y un lenguaje especializado en cada campo). La validez de los enunciados y principios morales que posibilitarán elaborar un texto informativo o prescriptivo, se apoya en la estrategia de la regla de la argumentación del "principio de universalidad" (U) que se concibe –desde la tradición habermasiana- como la idea común de no aceptar como moral más que normas admitidas por todos los posibles destinatarios y afectados mediante consenso intersubjetivo (Habermas, 2008, 74). Este principio, la universalidad como *moral point of view*, no actuaría mediante imperativos de cumplimiento moral, sino metodológicamente hacia la comprobación de la legitimidad y la validez de las máximas morales y jurídicas, reformulando incluso en su tentativa teórica el primer imperativo kantiano (imperativo categórico) desde una perspectiva dialógica y no monológica, es decir, desde la intersubjetividad del diálogo y no desde el *sujeto puro* presente en la ética kantiana. La validez del *deber ser* (obrar) no se manifiesta en la cualidad imperativa de una autoridad particular, sino en la de una *voluntad general* compartida por todos los afectados, que remite a un interés general determinable discursivamente, inteligible cognitivamente y visible desde la perspectiva de los participantes en la búsqueda del consenso a través del mejor argumento. A su vez, el modelo *pragmático universal* de Habermas muestra cómo en el "principio de universalización" (U) están implicados los presupuestos de la lógica y la argumentación. Para tal demostración se formulan unas determinadas reglas que responderían a la *esfera lógico-semántica, esfera pragmática-interaccional* y *esfera discursiva* (Habermas, 2008, 97-100):

1. *Esfera lógico-semántica* en la producción de argumentos que corresponden a una "lógica formal mínima" y carecerían de contenido moral:
   1.1. Ningún hablante debe contradecirse.
   1.2. Todo hablante que aplica el predicado F a un objeto *a* debe estar dispuesto a aplicar el predicado F a todo objeto que se parezca a *a* en todos los aspectos importantes.
   1.3. Diversos hablantes no pueden expresar la misma expresión con significados distintos.
2. *Esfera pragmática-interaccional* que consiste en la búsqueda cooperativa de la verdad a través de la argumentación como un procedimiento de en-

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

tendimiento donde entrarían normas de contenido ético que suponen relaciones de reconocimiento recíproco:

2.1. Cada hablante únicamente puede afirmar aquello en lo que verdaderamente cree.

2.2. Quien introduce un enunciado o norma que no es objeto de la discusión debe dar una razón para ello.

3. *Esfera discursiva* como proceso de argumentación que tiene que satisfacer condiciones improbables con vistas a lograr un acuerdo motivado racionalmente. En el discurso argumentativo se muestran estructuras de una "situación ideal de habla", inmunizada frente a la represión y la desigualdad:

3.1. Todo sujeto capaz de hablar y actuar puede participar en la discusión.

3.2. Todo sujeto puede cuestionar cualquier afirmación en el discurso. Introducir cualquier afirmación y manifestar sus posiciones, deseos y necesidades.

3.3. A ningún hablante puede impedírsele el uso de los derechos reconocidos en los dos primeros puntos anteriores (3.1-3.2) mediante coacción interna o externa al discurso.

En las reglas presentadas por Habermas se entrecruzan paralelamente la estructura formal de la *esfera lógico-semántica* con la *esfera pragmática-interaccional-discursiva* de producción de argumentos (de la proposición formal al juicio moral). Los últimos estudios sobre *teoría de la argumentación* han tenido una relevancia notable en las últimas décadas, resaltando la aplicación práctica de la misma en la década de los años ochenta por Hans-Hermann Hoppe (ética argumentativa). Por otra parte, la *Escuela de Lille* ha desarrollado desde la lógica dinámica un nuevo campo de estudio sobre dialógica: *lógica dialógica*. Siguiendo a la *Escuela de Erlangen* (Lorenzen y Lorenz), Shahid Rhaman y su equipo han logrado sistematizar la dialógica como *marco semántico*, con el fin de permitir el desarrollo y combinación de diferentes enfoques lógicos (lógica proposicional, lógica libre, lógica condicional, lógica normal e híbrida, lógica modal de primer orden, lógica relevante, etc.), que se traduce en un enfoque semántico-pragmatista de la lógica (Redmond y Fontaine, 2011). Estos últimos avances en dialógica pueden tener una relevancia notable en el transcurso dinámico de las éticas aplicadas, orientadas a *dar razones* y al consenso intersubjetivo.

A su vez, acompañando al "principio de universalización" (U) desde una visión dialógica, las éticas aplicadas, frente a las teorías éticas tradicionales, podrían

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

caracterizarse en cuatro rasgos exclusivos según la división presentada por Adela Cortina (Cortina, 2003, 21-23):

1. *Reflexión y lenguaje filosófico como elemento imprescindible de análisis.*
2. *Carácter prescriptivo limitado al no traspasar los umbrales de lo justo en su pretensión normativa* (no se entromete en los proyectos personales de vida plena).
3. *Carácter multidisciplinar* (elaboración realizada por todas las partes afectadas y expertos del campo, no solo por filósofos).
4. *"Pluralismo ético" como recurso indispensable*.

Los diferentes resultados obtenidos en el diálogo intersubjetivo se elaborarían en comités, reuniones o congresos, con la finalidad de elaborar un texto que tenga carácter prescriptivo, informativo o de *presión* democrática (o *lobby democrático*). La estructura de las éticas aplicadas seguiría el siguiente orden de desarrollo:

Diálogo interdisciplinar → Elaboración del texto → Publicación informativa o prescriptiva

2.2. La CiberÉtica como ética aplicada

En comparación con otras éticas aplicadas, la CiberÉtica está en proceso de maduración y precisa de una urgente implementación dentro de la filosofía moral y política. Como *pionero* de la CiberÉtica encontramos al padre la informática, el filósofo, matemático, lógico y criptógrafo Alan Turing (1912-1954). Además de proponer una influyente formalización de los conceptos de algoritmo y computación para encontrar un algoritmo general que decidiera, en lógica simbólica, si un fórmula de cálculo de primer orden es un teorema -la famosa "máquina de Turing", Turing trabajó en la formulación del concepto de hipercomputación y en la "máquina oracle", además de ayudar a descifrar los códigos "Enigma" en Bletchley Park, y ser considerado –junto a Norbert Wiener- uno de los desarrolladores de la *cibernética* como sistema de comunicación entre el hombre y la máquina mediante Inteligencia Artificial (Turing, 2010). En sus trabajos encontramos una reflexión sobre determinados problemas morales que surgen a raíz de sus investigaciones en Inteligencia Artificial, Vida Artificial, cibernética, *test de Turing*, etc. Después de Alan Turing la historia de la CiberÉtica ha implementado su campo de reflexión sobre todo en Estados Unidos, Europa y Australia:

> 1940-1950: *Norbert Wiener crea los estudios de* cibernética *en el MIT apoyándose en Alan Turing, observando las consecuencias sociales y éticas de este nuevo campo de estudio.*

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

1960: *Donn Parker (California) empieza a examinar las consecuencias éticas y legales en el uso de los ordenadores por usuarios e ingenieros.*

1970: *Joseph Weizenbaum (MIT) crea el programa ELIZA, uno de los primeros programas en procesar lenguaje natural (*bot *conversacional), y Walter Maner empieza a usar el término "Computer Ethics" en la Universidad.*

1980: *James Moor publica en 1985:* What is Computer Ethics?*, suponiendo un cambio de perspectiva en los estudios sobre CiberÉtica. En 1988 se empieza a preparar el I Congreso Internacional sobre CiberÉtica (realizado finalmente en 1991), reuniendo para la ocasión a filósofos, informáticos, sociólogos, psicólogos, abogados, economistas, periodistas y miembros del gobierno. A esta fecha hay que sumar la filosofía moral y política que lleva a cabo Richard Stallman con el proyecto s*oftware libre *(GNU/Linux), en contraposición a la filosofía de* software no libre *de Bill Gates (Microsoft) y Steve Jobs (Apple).*

1990: *Los problemas CiberÉticos llegan a Europa y Australia. Simon Rogerson establece en el Reino Unido el* Centre for Computing and Social Responsibility*, iniciando el ciclo de conferencias ETHICOMP. Surge el movimiento Cypherpunk (cuya cabeza visible sería el posterior fundador de WikiLeaks, Julian Assange) en la defensa del uso de la criptografía y otros métodos afines como medios para conseguir el cambio social y político. Este movimiento estuvo muy activo durante las "guerras criptográficas" de la década de los noventa y tras la* primavera virtual *de 2011 que incentivo el surgimiento de* Anonymous*. Destacar además la creación de la primera organización sin ánimo de lucro en la defensa de los derechos humanos digitales, la* Electronic Frontier Foundation *(EFF), con sede en San Francisco y con el apoyo de la ONU en la realización de documentos oficiales.*

2001- : *Los problemas CiberÉticos aumentan por diversos factores: los atentados del 11 S y la política de vigilancia masiva llevada a cabo por el gobierno americano (*Patriot Act*), el surgimiento de Industrias de la información y nuevas empresas tecnológicas como Google o Facebook -respaldadas por la tecnología del* Big Data*, las denuncias del matemático y exfuncionario de la NSA William Binney, las revelaciones de WikiLeaks, el gusano informático Stuxnet, las publicaciones de Edward Snowden, el* hacktivismo *presente en numerosos países del mundo, el activismo en red de usuarios particulares, la revolución tecnológica en todas las infraestructuras de los países, la información y la comunicación global, la interconexión total mediante los* smartphones *(*Android *de Google,* iOS *de Apple o* Windows Phone *de Microsoft), el* Internet de las cosas *(IoT), el cibercrimen o la ciberguerra, etc.*

Los análisis de los primeros *ciberéticos*, como James Moor, incluían la necesidad de observar la CiberÉtica en una triple división que incluyese (Spinello y Tavani, 2004, 2):

(a) una descripción de cómo las diferentes partes de la CiberÉtica han ido apareciendo en relación al avance tecnológico,

(b) una consideración de cómo existen problemas morales especiales en el campo de la cibertecnología, y

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 45-63

(c) la propuesta metodológica de ámbito aplicado para la investigación en CiberÉtica.

De igual manera que otras ramas de la ética aplicada precisan de un carácter interdisciplinar para la resolución de conflictos morales en un ámbito consensual, la CiberÉtica tiene un campo específico de acción. Al ser Internet y las tecnologías de la información un paradigma único en el tiempo que incide en todos los campos de la realidad social, entre los participantes del discurso aplicado en CiberÉtica podríamos encontrar: filósofos, economistas, programadores informáticos, auditores de seguridad, sociólogos, abogados, policías, militares, economistas, periodistas, hacktivistas, representantes de órganos institucionales del Estado, etc. Es la "globalización absoluta" de la ética aplicada (en una relación constante y necesaria entre sociedad civil y Estado), en un campo globalizado como es Internet y las nuevas tecnologías.

El deber de fomentar y ampliar valores morales se encuentra en el origen de las normas democráticas. Por ello es importante fomentar e implementar valores en los ámbitos aplicados, tal como señala la UNESCO en la *Declaración Universal sobre Bioética y Derechos Humanos*. Tomando como punto de partida los cuatro principios bioéticos clásicos de Tom L. Beauchamp y James F. Childress, desde la CiberÉtica se propone un anexo de cuatro principios según su ámbito aplicado. Los principios clásicos serían:

1. *Autonomía* (y libertad): Libertad del usuario en Internet y en el acceso a herramientas cibertecnológicas.

   Ejemplo: Los sistemas operativos Microsoft y Apple (*software no libre*), impiden al usuario conocer y modificar el *código fuente*. El usuario no tendría autonomía y libertad sobre el programa, sino que el programa (creado por el desarrollador) tendría el control sobre los usuarios (Stallman, 2004, 45-58).
2. *Beneficencia*: Obligación de actuar en beneficio de otros, promoviendo sus legítimos intereses y suprimiendo prejuicios.

   Ejemplo: En los diferentes casos de pedofilia digital se plantea la posibilidad de utilizar la figura jurídica del *agente encubierto*, herramienta policial especialmente eficiente para identificar y detener pedófilos que precisa de imágenes y otro tipo de material sensible para intercambiar con la red criminal y ganarse su confianza (Barrera, 2012).

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

3. *No maleficencia*: Abstenerse intencionadamente de realizar actos que puedan causar daño o perjudicar a otros.

   Ejemplo: Encontrar una *puerta trasera*[5] en un órgano institucional, universidad, empresa o ámbito doméstico, no debe dar lugar a realizar un *exploit*, esto es, acción de explotar una vulnerabilidad de un sistema a través de un fragmento de *software*, secuencia de comandos, datos, o acciones que permitan entrar ilícitamente en dicho sistema.

4. *Justicia*: Tratar a cada uno como corresponda, con la finalidad de disminuir las situaciones de desigualdad, ya sean de comunicación en red, *hardware* o *software*.

   Ejemplo: La interceptación por terceros de la información privada y las comunicaciones entre usuarios en red, supone un caso de injusticia social y comunicativa. Utilizar cifrado supone transformar un mensaje en texto normal, a texto cifrado o codificado mediante la verificación de las *fingerprints* y la clave pública PGP[6], las funciones *hash* y los certificados digitales.

A los principios clásicos, y desde los últimos avances llevados a cabo en ética aplicada, la complejidad de las tecnologías de la información precisa de cuatro nuevos principios a tener en cuenta:

5. *Sostenibilidad*: Comprobar y analizar el impacto tecnológico sobre la contaminación del suelo, la atmósfera, y el sistema de reciclado de materiales.

   Ejemplo: Con el aumento de las tecnologías de la información, los *smartphones* se están estableciendo en todas las sociedades a nivel global. El proceso de fabricación contiene, además de plástico y vidrio, una enorme cantidad de metales raros presentes en baterías, condensadores y pantallas como el paladio, el oro, la plata, el indio, el neodimio, el estaño, o el cobre (Valero Capilla, 2012, 24-27). A ello habría que sumar cuánta energía precisan los distintos *Big Data* para sostener la cantidad diaria de alrededor de 2,5 trillones de bytes de datos generados.

6. *Precaución*: Paralelamente al *principio de no maleficencia*, respalda la adopción de medidas de ciberseguridad y protección ante sospechas de que ciertas tecnologías puedan crear riesgo en el futuro.

   Ejemplo: El avance del *Internet de las cosas* (IoT) ha llevado a algunas empresas a dotar de *inteligencia*, conectividad y tecnología a los juguetes. El caso del osito de Fisher Price "Smart Toy Bear", ha saltado

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

todas las alarmas en ciberseguridad. Este juguete tenía en su interior un sistema operativo Android 4.4 –como el de los móviles, que podía ser reprogramado para modificar su uso. Esta nueva opción permitiría enviar videos e imágenes a un tercero, o utilizar el micrófono para realizar escuchas. También permitiría acceder a la plataforma de registro de clientes y conocer la edad, el nombre y el género del niño/a.

7. *Privacidad*: El usuario debe conocer los mecanismos de privacidad en red por su seguridad y anonimato, así como los sistemas de privacidad de *hardware* y *software*.

   Ejemplo: Según las revelaciones del ex agente de la NSA Edward Snowden, los principales servidores de Internet actuarían como proveedores de servicios para la NSA. El programa PRISM muestra como Microsoft, Yahoo!, Google, Facebook, PalTalk, AOL, Skype, YouTube y Apple, facilitan todos los datos de sus usuarios mediante *puertas traseras* (Greenwald, 2014, 134-135).

8. *Democracia*: Paralelamente al *principio de autonomía*, se debe promover en órganos institucionales una defensa de los Derechos digitales como Derechos Humanos, así como la ciberseguridad en infraestructuras domésticas, estatales, profesionales y críticas (hospitales, centrales nucleares, aeropuertos, suministros de agua, etc.)

   Ejemplo: Según el Departamento de Salud y Servicios Sociales de Estados Unidos (HHS), desde 2009 se ha accedido sin autorización y con ataques informáticos, al menos a los historiales médicos de veintiún millones de estadounidenses (Ungerleider, 2012). La facilidad de acceso a los sistemas de información implica la posibilidad de manipulación de historiales, así como el acceso a neveras de sangre, TACS, aparatos de Rayos X, equipos de anestesia, bombas de insulina, marcapasos, etc.

Afirmar desde la filosofía que el tipo de *saber práctico* propuesto por la CiberÉtica no encierra nada más que la novedad sobre problemas actuales, es no entender qué nos está ocurriendo –como sociedad interconectada a niveles globales- a comienzos del siglo XXI. Teniendo como base los cinco procesos indicados con anterioridad, se observa que desde la explosión tecnológica del *world wide web* de los años noventa (www), la línea ascendente de la *revolución digital* es a día de hoy imparable: destacar al respecto la creación del motor de búsqueda Google en 1998, Wikipedia en 2001,

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

la red de videos YouTube en 2005, la red social Facebook en 2005, Twitter en 2006, WhatsApp en 2010 o la novedad del *Internet of Things* (IoT) en 2015, entre muchos otros, hacen a día de hoy imposible negar el carácter transversal de la tecnología digital. Si a los avances tecnológicos indicados se suma la ascendente digitalización de todos los documentos oficiales de los Estados, revistas científicas, correos personales, adaptabilidad tecnológica de las infraestructuras estatales, domésticas y críticas (bolsa, centrales nucleares, hospitales, aeropuertos, depósitos de agua…), el cibercrimen en aumento, la ciberguerra entre Estados, la moneda digital *Bitcoin*, las revelaciones sobre la vigilancia de las comunicaciones, etc., la CiberÉtica es realmente el tipo de reflexión necesaria dentro del actual pluralismo cultural.

Por todo ello se propone una *nueva forma de saber*, de reflexionar sobre los problemas morales de las tecnologías de la información que lleven a recomendaciones para la acción. Son las sociedades interconectadas las que han exigido su nacimiento y actuación, son ellas las que precisan de este saber interdisciplinar para su acción en la vida pública (CiberPolítica), siendo un bien de primera necesidad para determinar la altura moral de una sociedad. Los estudios que se presentan sobre CiberÉtica a la Universidad y a diversos ámbitos de la sociedad civil, así como al Estado, estarían respaldados democráticamente, institucionalmente e inclusivamente por la Organización de las Naciones Unidas (ONU), concretamente por el Artículo 3, el Artículo 12 y el Artículo 19 de la *Declaración Universal de Derechos Humanos* de 1948. A los Derechos Humanos de *primera generación* (Derechos civiles y políticos), derechos de *segunda generación* (Derechos económicos, sociales y culturales), y derechos de *tercera generación* (Derechos ecológicos y de paz), habría que sumar los derechos de *cuarta generación*, que correspondería a los Derechos digitales: derecho a la libre expresión, derecho a la privacidad digital y la ciberseguridad, derecho al acceso al ciberespacio y a la información, derecho a asociarse en comunidades virtuales en Internet, derecho a tener Derechos digitales, etc. Veamos a continuación sus ámbitos de aplicación.

3. Áreas y subáreas de la CiberÉtica

La CiberÉtica, como podemos observar, surge a raíz de un conglomerado de problemas tecnológicos y filosóficos, presentes al final de la segunda guerra mundial y que

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

llegarían hasta nuestros días. Por ende, una clasificación sistemática sobre las áreas y subáreas de la CiberÉtica supone un punto de partida para abordar diferentes problemas que actualmente encontramos en la *sociedad red*.

Las principales áreas de la CiberÉtica corresponderían, por una parte, al soporte lógico-informático de las tecnologías de la información (*hardware* y *software*) presente en ordenadores, *smartphones*, tablets, IoT, etc., así como a otras variables no tecnológicas en relación con la tecnología. Estas áreas presentan algunas subáreas características a completar en el futuro.

- Hardware

1. Contaminación, reciclado de materiales tecnológicos y gasto de energía, en relación con el agotamiento de los recursos no renovables y el Cambio Climático.
2. *Hardware libre* (BIOS libre) y *hardware no libre*.
3. *Hardware* en infraestructuras domésticas, estatales, profesionales y críticas.
4. *Hardware* en el ámbito de la vida cotidiana.

- Software

1. *Software libre* (GNU/Linux) y *software no libre* (Microsoft y Apple): el problema del *código fuente*.
2. Ciberseguridad de los dispositivos contra ataques (privacidad, integridad, cifrado…).
3. *Software* en infraestructuras domésticas, estatales, profesionales y críticas.
4. *Software* en el ámbito de la vida cotidiana.

***Otras variables*:** Vigilancia de las comunicaciones, seguimiento de Industrias de la información al usuario en red con fines económicos, cibercrimen, ciberguerra, ciberterrorismo, hacktivismo, Derechos digitales, explotación infantil, *Internet of Things* (IoT), *smartcity,* legislación en red, *dark web*, identidad digital, gestión de la información, control parental, pederastia digital, trastornos psicológicos por el uso masivo de las TIC (iDisorder), geolocalización… y toda una lista interminable de variables y problemas que se presentan en numerosos casos prácticos.

Así como el Comité de Bioética de España (Ley 14/2007. Ministerio de Sanidad) tiene como una de sus funciones asesorar y emitir recomendaciones en materia de biomedicina e investigación, sería muy razonable por nuestra parte pensar sobre la

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

oportunidad de proponer la CiberÉtica como nuevo desarrollo paralelo en materia TIC e Internet, según la complejidad actual de las sociedades interconectadas en numerosos ámbitos de la realidad social.

4. Conclusiones: el *Manifiesto* de la ética hacker en seis principios

El término *hacker* tiene casi medio siglo de existencia. Su nacimiento se debe a las bromas que se gastaban los estudiantes del MIT en la década de los años sesenta del siglo pasado mediante los códigos de programación informática. Estas bromas, que llamaban "hacks", dieron lugar al término actual de *hacker* (Levy, 1984, 23). Con el paso del tiempo, los *hackers* del MIT fundaron el Laboratorio de Inteligencia Artificial (Ai Lab), donde se entusiasmaron por el *software libre* y la capacidad de transformar el mundo mediante la tecnología computacional, que permitía libre información, conocimiento y comunicación a través de la revolución que se estaba llevando paralelamente en microelectrónica y telecomunicaciones (ver apart. 1). Un ejemplo del trabajo realizado por aquellos ingenieros fue el llevado a cabo por Richard Stallman -al que aludimos con anterioridad. Su experiencia personal y conocimiento de los sistemas informáticos le llevó por primera vez a plantear la disyuntiva en torno al uso de *software libre*, que respetaría la libertad del usuario (GNU/Linux), o *software no libre*, que impediría transparencia y modificación del *código fuente* sin respetar la libertad del usuario (Microsoft y Apple), desde una perspectiva técnica, filosófica, sociológica y política. Un *filósofo* que procede del mundo de la programación informática, y cuyas ideas están detrás de todas las demandas que desde la opinión pública, periodistas, hacktivismo, WikiLeaks, Edward Snowden o la *Electronic Frontier Foundation* (EFF), se llevan a cabo para defender una mejor privacidad del usuario, libertad, democracia, comunicación libre, información, transparencia, tecnología basada en un uso eficiente de los recursos y en el reciclado de materiales, etc. (Romero, 2017).

Por todo ello, es erróneo sentenciar a los *hackers* como delincuentes o "piratas" del ciberespacio y, peor aún, considerarlos como tales desde las universidades, colegios, instituciones públicas, Estados o documentos oficiales de la lengua de un país, como en el caso español del diccionario de la Real Academia Española (RAE), que en su vigesimotercera edición de 2014 identifica al hacker como "pirata informático". Ser

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 45-63

hacker es un orgullo, y aunque se suele caracterizar peyorativamente, *un hacker* sería, según la aprobación mayoritaria del término en 1983 por la prestigiosa organización internacional IETF (Internet Engineering Task Force), toda persona, perteneciente al mundo informático y de las telecomunicaciones, con gran cantidad de conocimientos tecnológicos sobre el funcionamiento interno de un sistema operativo, de una red de ordenadores, Internet o cualquier tecnología, que llevaría su uso al límite (Scott Malkin y LaQuey Parker, 1983). Al ser un término polisémico, el uso que se haga del mismo puede caracterizarse como:

- *White hat* (seguridad informática y determinadas agencias del Estado),
- *Grey hat* (hacktivismo),
- *Black hat* (cibercriminales o *crackers*), y
- *Lamer* (no hacker. Persona que utiliza herramientas de *hacking* sin ser hacker. Puede actuar a partir de los tres anteriores: *lamer White hat, lamer Grey hat* y *lamer Black hat*).

La filosofía hacker ha tenido como fin desde sus inicios en el MIT la libertad de información y de conocimiento entre todas las partes dinámicas del mundo por el *bien común* de la comunidad (humanidad) interconectada. Hoy en día, para evitar recaer en la identificación de hacker con *cracker* (cibercriminal), la *comunidad hacker* respalda seis principios presentados al modo de una ética hacker por Steven Levy en 1984. Estos principios, que pueden leerse como un *Manifiesto*, y que responden a la "forma de vida", en sentido wittgensteiniano, de una ética inamovible en un sistema dinámico como es Internet, serían los siguientes (Levy, 1984, 39-49):

1. El acceso a los ordenadores –y cualquier cosa que pueda enseñar algo acerca de la forma en que funciona el mundo- debe ser ilimitado y total.
2. Toda información debe ser libre.
3. Es necesario promover la descentralización –y desconfiar de los poderes establecidos.
4. Los *hackers* deberían ser juzgados por su labor y capacidad, no por criterios como raza, edad, sexo o posición.
5. Se puede crear arte y belleza en un ordenador.
6. Los ordenadores pueden cambiar tu vida para mejor.

Estos seis principios propuestos por Steven Levy son reconocidos por la mayoría de los hackers, que incorporan dicha ética a su "forma de vida". Ahora es momento de observar, reflexionar y analizar las tecnologías de la información desde todos

los campos del saber humano, más allá de la *tecnofobia* y la *tecnofilia*, es decir, desde una postura crítica (*tecnocrítica*), raíz del pensamiento filosófico que desde la CiberÉtica se presenta. Si bien los últimos avances en filosofía han concluido, tras las revelaciones conocidas desde la teoría evolutiva y los avances en inteligencia artificial (IA) y computación, que lo que nos distingue como criaturas racionales y lógicas es el *lenguaje* y la información transmitida por esta facultad humana (Brandom, 1994), en la *era digital* se precisa de un conocimiento mayor sobre las nuevas formas de transmitir información, que han cambiado, cambian y cambiarán nuestras vidas. La lechuza de Minerva, símbolo de la diosa de la sabiduría en épocas antiguas, atrapa al *glider*[7] con sus garras, y parece que el planeo dinámico lo harán juntos durante largo tiempo.

Bibliografía[8]

Barrera, Silvia. (2012): "La lucha del Cuerpo Nacional de Policía contra las redes organizadas de pedofilia", en: *Seguridad Pública: retos actuales y perspectivas de futuro*. Madrid, Seguridad y Ciudadanía, 7-8, Revista del Ministerio del Interior, pp. 101-123.

Brandom, Robert. (1994): *Making it Explicit. Reasoning, Representig, and Discursive Commi tment*. Cambridge, Cambridge, Harvard University Press.

Castells, Manuel. (1998): *La era de la información. Vol.1*. Madrid, Alianza Editorial.

Cortina, Adela (2003): "El quehacer público de las éticas aplicadas: ética cívica transnacional", en: Adela Cortina y Domingo García-Marzá (eds.), *Razón pública y éticas aplicadas. Los caminos de la razón práctica en una sociedad pluralista*. Madrid, Tecnos.

Greenwald, Glenn (2014): *Snowden. Sin un lugar donde esconderse*. Barcelona, Ediciones B.

Habermas, Jürgen (2000): *Aclaraciones a la ética del discurso*. Madrid, Trotta.

Habermas, Jürgen (2008): *Conciencia moral y acción comunicativa*. Madrid, Trotta.

Levy, Steven. (1984): *Hackers. Heroes of the computer revolution*. New York, A Delta Book.

Redmond, J. y Fontaine, M., (2011): *How to Play Dialogues. An Introduction to Dialogic Logic*. London, College Publication.

Romero, Javier. (2017): "Democracia y *software libre*: el soporte lógico-informático de las políticas deliberativas", en: Ramón Cotarelo y Javier Gil (comps.), *Ciberpolítica: Gobierno abierto, redes, deliberación, democracia*. Madrid, INAP, pp. 78-87.

Scott Malkin, G. y LaQuey Parker, T., (1983): *Internet Users´ Glossary*. Internet Engineering Task Force (IETF), en: https://tools.ietf.org/html/rfc1392

Spinello, Richard. A. y Tavani, Herman. T. (2004): *Readings in CyberEthics*. Toronto, Jones and Bartlett Publishers.

Stallman, Richard M. (2004): *Software libre para una sociedad libre*. Madrid, Traficantes de sueños.

ISSN 1989-7022 DILEMATA, año 9 (2017), nº 24, 45-63

ISSN 1989-7022

Turing, Alan. (2010): *The Essential Turing. Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life plus The Secrets of Enigma,* (edited by B. Jack Copeland). Oxford, Oxford University Press.

Ungerleider, Neal. (2012): "Medical Cybercrime: The Next Frontier", en: *Fast Company*.

Valero Capilla, Antonio. (2012): *Evaluación del agotamiento del capital mineral de la Tierra. Más allá del Cambio Climático*. Zaragoza, Prensas de la Universidad de Zaragoza.

Web oficiales de organismos públicos, España:

AEPD (Agencia Española de Protección de Datos): www.agdp.es

BIT (Brigada de Investigación Tecnológica) Policía Nacional: www.policia.es/org_central/judicial/udef/bit_alertas.html

CCN (Centro Criptológico Nacional) Centro Nacional de Inteligencia: www.ccn.cni.es

CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas) Ministerio del Interior: www.cnpic.es

GDT (Grupo de Delitos Telemáticos) Guardia Civil: www.gdt.guardiacivil.es

INCIBE (Instituto Nacional de de Ciberseguridad): www.incibe.es

MCCD (Mando Conjunto de Ciberdefensa): www.emad.mde.es/CIBERDEFENSA/

Notas

1. La *teoría del caos* analizada desde la *teoría de sistemas*, dentro de las matemáticas, la física, la biología, la economía, la informática o la meteorología, muestra la interdependencia entre los diferentes sistemas al observar cómo a partir de un sistema caótico, cualquier pequeña divergencia entre dos situaciones con una variación pequeña en los datos iniciales, podría acabar dando lugar a situaciones donde ambos sistemas evolucionarían de forma diferente y sin la posibilidad de analizar las consecuencias globales.

2. La IP se caracteriza como la numeración única de 32 bits que todo sistema operativo posee en red.

3. Ver al respecto: www.internetworldstats.com/stats.htm

4. Existe en verdad una recopilación de artículos sobre la relación de los Derechos Humanos y las nuevas tecnologías, ver: González R. Arnaiz, G (coord.), (1999). *Derechos humanos. La condición humana en la sociedad tecnológica*. Madrid, Tecnos. Por lo demás encontramos pequeñas reflexiones con escaso conocimiento técnico desde el campo filosófico, bien desde una *tecnofobia* dominante, o desde una *tecnofilia* presente en determinados análisis filosófico-políticos y sociales, sin dejar de lado la recogida de datos sociológico-estadísticos desde la filosofía social de la ciencia.

5. Una *backdoor* es una vulnerabilidad de software que permite a un usuario o fabricante introducirse en sistemas informáticos ajenos. También pueden llamarse *bug* o *holes*.

6. El cifrado PGP (Pretty Good Privacy) es el sistema más utilizado por los *hackers* para cifrar las comunicaciones, utilizando una combinación de claves públicas y privadas de hasta 2.048 bits. Por citar un ejemplo, con 200 dígitos se realizan $1{,}2x10^{23}$ operaciones con un tiempo de descifrado en ataque de $3{,}8x10^{9}$ años en sistema de cifrado clásico RSA. Hay una versión de cifrado desde los postulados filosóficos de la *Free Software Foundation*: GnuPG ID.

ISSN 1989-7022

7. El *glider* es el emblema más reconocido por los hackers. Propuesto en 2003 por Eric S. Raymond, su objetivo es unificar en un símbolo reconocible la percepción de la cultura hacker. El uso de este símbolo pretende alejarse de los *crackers*, expresando la solidaridad con los objetivos y valores éticos de los hackers, y la forma de vivir de un hacker. Su imagen es la representación de un planeador, un autómata celular diseñado por el matemático John Horton Conway en 1970, que equivale a "la máquina universal" de Alan Turing, es decir, todo aquello que se puede computar algorítmicamente, se puede computar en el *juego de la vida* como emergencia y autoorganización. Con ello se puede observar cómo determinados patrones complejos pueden originarse a partir de la implementación de reglas muy sencillas.

8. El desarrollo del siguiente artículo tenía que beber directamente de las fuentes hechas a base de unos y ceros (1,0), además de las numerosas charlas y jornadas en distintas CON españolas y congresos de ciberseguridad de las que llevo asistiendo largo tiempo. Mi experiencia y amistad con diferentes *hackers*, y mi cooperación con el INCIBE (Instituto Nacional de Ciberseguridad) y el OSI (Oficina de Seguridad del Internauta), forman parte de mis conocimientos sobre el desarrollo de la CiberÉtica. Agradecer a la Fundación Tatiana Pérez de Guzmán el Bueno por su confianza y apoyo.

DILEMATA, año 9 (2017), nº 24, 45-63