Universitat Autònoma de Barcelona

La privacidad en el ciberespacio. Una aproximación filosófica en el entorno digital a partir de un estudio de caso sobre el buscador Google

Ana María Arconada Beasoain de Paulorena

TESIS DOCTORAL de

Ana María Arconada Beasoain de Paulorena

Dirigida por

David Casacuberta

La privacidad en el ciberespacio

Una aproximación filosófica en el entorno digital
a partir de un estudio de caso sobre
el buscador Google

Doctorado en Filosofía - Departamento de Filosofía

Universidad Autónoma de Barcelona

2016

Agradecimientos

Esta investigación es el trabajo de muchos. Debo dar las gracias a todos y todas.

En especial quiero dar las gracias y dedicar esta investigación a mi madre. Ella ha sido y será el ejemplo de mi vida. Me enseñó el valor del esfuerzo desde la humildad. Me enseñó a ser fuerte a pesar de las dificultades. Me demostró, a través del ejemplo, que nada nos separa de lo que queremos ser salvo nosotras mismas.

Debo dar las gracias a mis hermanos, por haberme obligado, con cariño, a escribir todos aquellos juegos en el 48k.

Debo dar las gracias a David. Siempre ahí, siempre positivo, siempre con una palabra amable, constructiva. ¡Seguimos!

Debo dar las gracias a mis amigos y amigas. A los que preguntaron, por su interés. A los que no preguntaron, porque sabían que no era el momento.

Debo dar las gracias a César. Lector, crítico, amigo y compañero.

La privacidad en el ciberespacio

Una aproximación filosófica en el entorno digital
a partir de un estudio de caso sobre
el buscador Google

ÍNDICE

INTRODUCCIÓN:
PREGUNTAS DE INVESTIGACIÓN
Y METODOLOGÍA

Los ordenadores personales, Internet, la telefonía móvil y los *smartphones* o las videollamadas, tan presentes en la vida cotidiana de las personas que cuesta recordar aquella época en la que toda esa tecnología formaba parte de la ciencia ficción. Los nativos digitales preguntan con curiosidad a los inmigrantes digitales[1] cómo eran las comunicaciones por entonces, cómo se mantenían conectados, qué tipo de relaciones tenían, como si estuvieran preguntando al medieval cómo podían ir de un sitio a otro sin la existencia de coches o aviones. Las personas de la tercera edad miran con estupor cómo sus nietos y nietas viven en un mundo que no comprenden, que ya no es el suyo. Los pequeños, por su parte, no pueden entender una existencia alejada de todos esos dispositivos y herramientas y observan a sus mayores con la incredulidad del experto ante el neófito.

Las tecnologías digitales han traído consigo, además de la brecha digital entre generaciones, la necesidad de replantear las formas de habitar el mundo, el modo en que las personas se relacionan y conviven. En todas las épocas ha habido cambios que han llevado a que las generaciones anteriores y presentes se vean diferentes las unas a las otras, y lo que para unas era lo habitual para otras es extraño. Sin embargo, en el tiempo presente, tanto unas como otras comparten esos cambios. Unos cambios que deben ser atendidos ya que alcanzan todos los aspectos de la vida.

Con mayor o menor rapidez, más o menos éxito, las diferentes ciencias y disciplinas se han ido adaptando al cambio y han asumido el nuevo medio. Para muchas, las tecnologías digitales han supuesto un avance y desarrollo sin precedentes. La posibilidad de análisis, almacenamiento y transmisión de información ha beneficiado a todos los ámbitos científicos. La creación de nuevas y mejores herramientas digitales ha significado un gran salto para la realización de trabajos manuales y mecánicos. Las comunicaciones digitales han posibilitado la difusión, el reparto y la transmisión de conocimiento.

La filosofía, como todas las ciencias humanas, también ha tenido que adaptarse a este nuevo espacio social y humano. Aparecen nuevas preguntas o se reformulan viejas cuestiones desde puntos de vista novedosos. La creación de nuevas formas de inteligencia, la expansión de la memoria más allá de la biológica, la aparición de artefactos con los que los humanos se relacionan o el surgimiento de elementos que necesitan ser explicados filosóficamente, son algunas de las novedades que han traído las tecnologías digitales al pensamiento filosófico. Para ello, la filosofía

---

[1] Lo nativos digitales son las personas nacidas después de 1980, cuando las tecnologías digitales estaban relativamente avanzadas. Por su parte, los inmigrantes digitales son aquellas nacidas entre 1940 y 1980 que, habiendo nacido en un mundo analógico, tuvieron que aprender a vivir en este nuevo entorno (Prensky, 2001)

tiene que desarrollar nuevos discursos, nuevas herramientas y nuevas formas de expresión que le permitan aprehender y analizar estos elementos, asimilarlos como suyos y devolverlos, al exterior, criticados. Esta investigación se enmarca en ese quehacer filosófico.

Uno de los temas que atañe a la filosofía respecto a las tecnologías digitales está relacionado con ese espacio social que se ha creado en torno a éstas, denominado ciberespacio. Se puede definir el ciberespacio como el ámbito creado artificialmente por medio de sistemas informáticos. Sin embargo, esta definición no parece ajustarse a la realidad, ya que el ciberespacio es algo más que un medio no natural electrónico. Bruce Sterling lo define como:

> El ciberespacio es el lugar en el que una conversación telefónica parece tener lugar. No en el interior de tu teléfono, el dispositivo de plástico de tu mesa. No en el interior del teléfono de la otra persona, en otra ciudad. El lugar entre los teléfonos. El lugar indefinido de ahí fuera, donde vosotros dos, dos seres humanos, os encontráis y os comunicáis. Aunque no es exactamente real, el ciberespacio es un lugar que existe. Hay cosas que ocurren allí que tienen consecuencias muy reales. Este lugar no es real, pero es serio, es importante.
> (Sterling, 1999, p. 16)

Aunque el término procede de la ciencia ficción[2], éste ha sido acuñado para referirse a todo aquello que sucede en este entorno digital y al cual se accede a través de tecnologías digitales. El ciberespacio es el lugar donde Internet ocurre. Internet es un conjunto descentralizado de redes que permite la comunicación entre dispositivos alejados entre sí y no conectados físicamente, y esa comunicación se da en el ciberespacio.

La filosofía, por lo tanto, se encargará de analizar las cuestiones filosóficas que surjan en ese medio. Como medio de interacción humana, entre los problemas que deberá afrontar estarán aquellos que tienen que ver con la ética y la moralidad de las acciones humanas desarrolladas en este entorno. Este campo de actuación será donde se desarrolle y despliegue la ciberética. Ésta se puede definir como:

---

[2] El término apareció por primera vez en la novela *Neuromancer* escrita por William Gibson en 1984.

> The field of applied ethics that examines moral, legal, and social issues in the development and use of cybertechnology. Cybertechnology, in turn, refers to a broad spectrum of technology that range from stand-alone computers to the cluster of networked computing, information, and communication technologies.
> (Spinello, Tavani, 2004, p. 1)

El campo de estudio de la ciberética es amplio y diverso. Abarca, entre otras cosas, el diseño de los artefactos o dispositivos, los motivos que operan tras ese diseño, el uso que el ser humano pueda darles, esto es, la relación final entre éste y la máquina, y las posibles consecuencias de ese uso. Dicho de otro modo, entre sus preocupaciones principales se encuentran las relacionadas con el mejor modo de actuación en relación a las tecnologías digitales; las normas que deben considerarse como apropiadas; en virtud de qué valores se persiguen y plantean esas normas o con qué finalidad se llevan a cabo. Como espacio multicultural, la ciberética se encarga también de establecer pautas que permitan gestionar la diversidad dentro de un único espacio que es el ciberespacio.

En virtud de este abanico tan amplio, la ciberética implica la presencia de diversos actores, tales como diseñadores, programadores, informáticos, productores, comercializadores, usuarios finales, etc. Esta diversidad de puntos de vista desde los cuales se puede abordar la ciberética implica que existan, a su vez, una variedad de acepciones para ella. Así, es posible encontrar términos que, a pesar de contener diferencias, suelen tenerse como sinónimos. Conceptos como ética informática, relacionada con el diseño de artefactos tecnológicos, ética computacional, referida a las cuestiones derivadas de la programación, ética de Internet o ciberética, encaminadas al análisis de las cuestiones relativas a Internet, abarcan todos estos puntos de vista desde los cuales se tratan las cuestiones éticas referidas a los artefactos tecnológicos y el ciberespacio. Esta investigación se enmarca dentro de la ética de Internet o ciberética.

Esta investigación parte del supuesto de una migración masiva hacia el ciberespacio. Migración que se ha dado de un modo involuntario y progresivo. Involuntario porque no se ha realizado de un modo consciente y articulado. La progresiva migración ha dificultado la aprehensión de los cambios que ha supuesto para los modos de vida, las personas y la sociedad en general. Desde esta perspectiva se mostrará como esa dificultad de adaptación al nuevo contexto ha significado una

situación de fragmentación, donde las tecnologías digitales, la filosofía en general y la ética en particular, así como los seres humanos, no han avanzado al mismo ritmo ni en la misma dirección hacia la construcción de este espacio social.

Se mostrará que esa falta de conexión o asincronía entre los agentes involucrados ha significado que cada uno de ellos adopte diversas posturas a la hora de crear marcos de referencia para este nuevo espacio social. Las tecnologías digitales, representadas en esta investigación por las empresas productoras del ciberespacio y en el caso concreto por Google, han desarrollado y construido esta "aldea global" bajo sus propios criterios y en virtud de sus propios intereses. Por su parte, la filosofía y la ética no parecen tener la suficiente capacidad de avanzar hacia un plano teórico aplicado, fundamental para este nuevo medio. Finalmente, los ciberciudadanos, sin apoyo de las instituciones ni de marcos filosóficos que los guíen, intentan habitar este nuevo espacio a través de la adaptación al medio.

Se afirmará la centralidad de la privacidad como problema fundamental donde no existe acuerdo entre estos tres actores del ciberespacio, de ahí que sea el objeto principal de estudio de esta investigación. Desde una perspectiva transversal se atenderá a las diferentes formas que toma la privacidad para estos tres agentes principales.

Desde el análisis de Google se mostrará cómo la información del usuario supone para la empresa su mayor fuente de ingresos. Los servicios gratuitos que ofrece a los usuarios vienen determinados por la gestión exclusiva de esa información. Por ello, se mostrará cómo Google tiene un amplio interés en mantener la información dentro de cierto ámbito privado, siendo ésta aquello que le permite estar en una posición dominante dentro de las tecnologías digitales en el ciberespacio.

Por otra parte se propondrá como problema fundamental de la filosofía, y en concreto de la ciberética, a la hora de abordar la cuestión de la privacidad, una conceptualización basada en presupuestos que dificultan la creación de un corpus ético que sea válido para este nuevo espacio social. Se afirmará que esa privacidad, aquí denominada "privacidad analógica", padece de tres defectos fundamentales, a saber: 1) el mantenimiento de la dicotomía entre espacio público y privado; 2) descontextualizada del lugar donde se desarrolla y debe aplicarse; y 3) alejada de las decisiones que los propios usuarios toman a la hora de abordar su propia privacidad.

Desde el punto de vista del usuario se atenderá a la distinción propuesta por Manuel Castells entre productores-usuarios y consumidores-usuarios. “Por productores/usuarios me refiero a aquellos cuyo uso de Internet retroalimenta al sistema tecnológico, mientras que los consumidores/usuarios son aquellos receptores de aplicaciones y sistemas que no interactúan directamente con el desarrollo de Internet” (Castells, 2001, p. 51). Se examinará cómo Google mantiene una relación desigual con estos dos grupos de usuarios con intereses contrapuestos, lo que lleva a mantener relaciones éticas también contradictorias. La información concebida como privacidad de los consumidores es utilizada por Google para obtener beneficios permitiendo el acceso a esa información a los productores, que comercializan productos basados en los intereses y en modelos de usuario que Google obtiene de los consumidores al utilizar éstos sus servicios. Los usuarios-compradores, a su vez, se benefician de los servicios que Google les ofrece de forma gratuita, aceptando las condiciones de uso por los servicios prestados, sin atender a las posibles consecuencias sobre la información que dejan en la red.

Se explicarán las diversas posturas éticas que abordan el tema de la privacidad en el ciberespacio y se analizarán estas posiciones desde la Política de privacidad de Google. Con ello ser verá cómo estas posturas no acaban de responder a las cuestiones planteadas en este nuevo espacio respecto a la privacidad. Desde el punto de vista de Google se mostrará como la empresa mantiene una postura cercana a todas estas teorías éticas pero que, paradójicamente, debe alejarse de todas ellas para mantener su propia existencia y parte de la estructura actual del ciberespacio. Se observará cómo determinados aspectos de Internet vienen determinados por la gestión de la información de los usuarios y cómo esa gestión es fundamental para ofrecerles servicios.

Se verá cómo la existencia de dos grupos de usuarios determina el comportamiento de Google ante la privacidad de la información. Mientras desarrolla productos, servicios y políticas de privacidad encaminadas a entender la privacidad de los consumidores-usuarios como un valor fundamental a salvaguardar en el ciberespacio, por otra parte produce una línea de productos y servicios, dirigidos a los productores-usuarios, basados en el acceso a la información de los primeros. Sin embargo, como se intentará mostrar, las consecuencias de esta gestión de la información maximizan el bienestar general en la medida en que unos y otros obtienen los productos y servicios deseados.

Por último se analizarán y sopesarán las ventajas e inconvenientes de adoptar una nueva perspectiva para el concepto de privacidad. Se intentarán mostrar los beneficios de una definición de privacidad

digital frente a una analógica y se propondrá una definición de privacidad digital que conserve los derechos de los ciberciudadanos y que continúe permitiendo la estructura actual del ciberespacio.

El concepto de ética esgrimido en esta investigación se apoya en la idea de una ética aplicada. Para su definición se tendrá en cuenta las ideas de Peter Singer planteadas en su obra *Ética práctica* (1980). Una ética que quiera servir, en tanto funcionar, debe poderse aplicar al mundo. "Un juicio ético que no sea válido en la práctica debe padecer a la vez un defecto teórico, ya que la razón principal de todo juicio ético es servir de guía a la práctica" (Singer, 1984, p. 2)

Una ética normativa lleva consigo la dificultad de no poder hacer frente a las circunstancias, en la medida en que no tiene en cuenta las particularidades de cada situación en las que se va a tener que aplicar. Es cierto que se puede pensar que precisamente eso es la ética, un conjunto de normas y valores que se han de respetar con independencia de cuales sean las situaciones en las que se tenga que aplicar. Sin embargo, este tipo de ética corre el riesgo de entrar en conflicto consigo misma.

Cuando sea necesario dejar el plano teórico y deba aplicarse a la vida diaria es posible y probable que deba introducir una excepción para la norma a modo de jerarquía ética vertical, donde cada norma tiene a su vez su excepción o subnorma, para dar respuestas a casos excepcionales. El ejemplo de las mentiras es un caso clásico sobre el problema de la normatividad de la ética. Ejemplo que no deja de plantear Singer al afirmar que *"*puede que normalmente sea malo mentir, pero si estuviéramos viviendo en la Alemania nazi y la Gestapo tocara a la puerta buscando judíos, seguramente estaría bien negar la existencia de la familia judía que se esconde en el ático" (Singer, 1984, p. 3)

Se ha creído conveniente entonces que, en la medida en que el ciberespacio es un lugar siempre en movimiento y cambiante, compartido por multitud de agentes que provocan situaciones, esta investigación tenga su base en una ética aplicada. Es necesario un enfoque ético que pueda hacer frente a las cuestiones planteadas por la ciberética sin el constreñimiento de una ética teórica del tipo "esto está bien" o "esto está mal" que no tenga en cuenta sus particularidades. Para ello,

> Existe un enfoque tradicional de la ética que se ve poco afectado por las cuestiones complejas que hacen difícil la aplicación de las normas simples: se trata del punto de vista consecuencialista. Los consecuencialistas no empiezan con las normas morales sino con los objetivos. Valoran los actos en función de que favorezcan la consecución de estos objetivos.
> (Singer, 1984, p. 3)

Cabe siempre la posibilidad que al hablar de particularidades dentro de la ética éstas se entiendan como una pretensión al relativismo, y que el resultado final sea desembocar en una ética basada en intereses personales y por tanto alejada de maximizar el bien común. Sin embargo, no es la intención del consecuencialismo, como tampoco lo es de esta investigación, el intentar amoldar la ética a cada situación de modo que se pueda actuar libremente en cada caso particular. El consecuencialismo, y su teoría más desarrollada el utilitarismo, sostienen que "[...] un principio ético no se puede justificar en relación a un grupo particular o parcial dado: la ética requiere un punto de vista universal, lo cual no quiere decir que un juicio ético deba ser universalmente aplicable" (Singer, 1984, p. 14).

Al ser este un estudio sobre Internet, que por definición tiene un carácter global, es necesaria una ética de este tipo que sea capaz de realizar juicios éticos de carácter universal al tiempo que tenga en cuenta cada caso en particular.

> La postura utilitarista es una postura mínima, una primera etapa que alcanzamos al universalizar la toma de decisiones interesada. Si vamos a pensar de forma ética, no podemos negarnos a dar este paso. Si nos vamos a persuadir de que debemos ir más allá del utilitarismo y aceptar ideales y normas morales no utilitaristas necesitamos contar con buenas razones para dar este paso hacia adelante.
> (Singer, 1984, p.18).

La ética no debe quedarse atrás en cuanto a la tecnología y los posibles cambios derivados de ella. Es necesario abordar las cuestiones relativas a las telecomunicaciones y en concreto al ciberespacio de un modo ético aplicado, explorar los posibles cambios y las nuevas cuestiones que de ella se desprendan. Si la ética no es capaz de incluirse en el discurso tecnológico es poco probable que se la tenga en cuenta dentro de la discusión. Si bien es cierto que a medida que se desarrollan los

avances tecnológicos queda más patente la necesidad de una ética que los critique, los avale, los supervise y los controle, también es cierto que si se cede esa formulación a las mismas empresas productoras de la tecnología, se corre el riesgo de producir una ética amoldada a sus necesidades. Un ejemplo es ahora oportuno a este respecto.

Google tiene un amplio documento, público y abierto a todos los usuarios, donde éstos pueden ver qué hace la empresa para mantener la privacidad y la seguridad de la información de éstos. Material que será utilizado a lo largo de esta investigación. En un apartado titulado "Tu contenido en nuestros Servicios" Google afirma que toda la información almacenada en sus servicios seguirá siendo propiedad del usuario que la haya generado, como dicen: "en pocas palabras, lo que te pertenece, tuyo es". Se entiende entonces que Google defiende la propiedad intelectual de la información de los usuarios y que, al menos en este sentido, es defensor de una ética en Internet. El problema viene en el apunte que hacen más bajo sobre esta propiedad. El documento continúa, "al subir, almacenar o recibir contenido o al enviarlo a nuestros Servicios o a través de ellos, concedes a Google (y a sus colaboradores) una licencia mundial para usar, alojar, almacenar, reproducir, modificar, crear obras derivadas, comunicar, publicar, ejecutar o mostrar públicamente y distribuir dicho contenido"[3]. En otras palabras, lo que es tuyo se convierte en propiedad de Google.

En este ejemplo se observa que Google está respondiendo a unas demandas encaminadas a salvaguardar los derechos de los usuarios y por tanto, está actuando con cierta ética. Ahora bien, estas acciones no son suficientes en la medida en que, al tiempo que manifiesta un respeto por la propiedad intelectual de la información obliga al usuario a ceder esa información para poder hacer uso de los servicios que ofrece. Esto viene a decir que para poder utilizar sus servicios se tiene que, de algún modo, ceder derechos de propiedad intelectual a la empresa. Son casos como este los que ponen de manifiesto la necesidad de una ética que regule o fuerce a las compañías, los gobiernos y la opinión pública a establecer unas normas de comportamiento en el ciberespacio y en concreto en Internet.

Las citas aparecidas en esta investigación se mantendrán en el idioma de las fuentes consultadas, por lo que habrá citaciones en inglés y en castellano. En la bibliografía se hará referencia a las obras originales o a la traducción, y traductor, cuando sea necesario

[3] https://www.google.es/intl/es/policies/terms/regional.html

CAPÍTULO 1:
CIBERÉTICA. UNA HISTORIA MUY CORTA

La ética informática, en comparación con otras éticas, es una disciplina muy reciente. Tiene su origen a mediados del siglo veinte, cuando la tecnología y las comunicaciones se desarrollan a gran velocidad y a escala mundial, debido en parte a la Segunda Guerra Mundial. Es en este contexto bélico y en concreto en el seno de la propia comunidad de profesionales encargados de desarrollar esta tecnología donde aparece el germen de esta nueva ética.

En 1948 Norbert Wiener, profesor de matemáticas en el MIT, publica *Cibernetics: Or Control and Communication in the Animal and the Machine*, una obra donde se analiza los nuevos elementos éticos que suponen las tecnologías de la comunicación. En palabras del autor, "Cybernetics takes the view that the structure of the machine or of the organism is an index of the performance that may be expected from it" (Wiener, 1985, p. 57).

La combinación de la capacidad performativa del ser humano y la de la máquina son el punto de partida de estos nuevos aspectos éticos. La capacidad "ilimitada" de las nuevas tecnologías supone para el ser humano una puerta abierta a sobrepasar sus limitaciones: la comunicación a distancia; el intercambio de bienes y servicios sin presencia física de las partes; la consulta y el tratamiento de enfermedades sin acudir a un centro de salud; la violencia o guerra contra personas o lugares remotos, etc.. Hasta la aparición de las tecnologías digitales estas acciones habían requerido de la presencia humana para su realización. Era necesaria la presencialidad humana para llevarlas a cabo. Con las tecnologías digitales es posible relegar estas acciones a las máquinas. Programarlas para realizar casi cualquier tarea. La cuestión radica, y así lo entiende la ciberética, en saber qué se quiere, puede y/o debe delegar a las máquinas, qué aspectos de la vida humana pueden dejarse al computo matemático, a los algoritmos, qué consecuencias pueden surgir de esa vida computacional y qué consecuencias pueden derivarse de su uso.

Uno de los aspectos que plantea la revolución de las comunicaciones a la ética tradicional tiene que ver con los fundamentos mismos de la ética. Hasta el momento la ética había tenido unos objetivos claros. Moviendo sus límites, fundamentos o aspectos, pero basados en cuestiones siempre iguales, tales como la justicia, el bien, lo correcto, etc. Las diferentes escuelas de pensamiento ético se distinguían entonces en el acento que ponían a las diversas variables que componían su discurso, variables que se mantenían en el tiempo a pesar de los cambios de perspectiva.

Con la ética informática surge la pregunta de si toda esta tecnología, que cambia de un modo tan rápido las interacciones entre las personas y la tecnología, no cambiará, o al menos afectará, a su vez, otros aspectos de la sociedad incluida la ética y sus fundamentos. De hecho, es necesario, y objeto de este estudio, reflexionar sobre el alcance de la ética en Internet, ya que "la tecnología se convierte en portadora y transmisora de interpretaciones de la realidad y, por tanto, de valores" (Feltrero, 2006, p. 90). La ética, por lo tanto, debe avanzar hacia el análisis y comprensión de estos nuevos marcos, su objetivo debe ser "la búsqueda de una definición de la singularidad de este campo de reflexión ética" (Feltrero, 2006, p. 80).

Unos interrogantes que plantean inquietud a la hora de abordar los avances tecnológicos vienen determinados por la rapidez misma con la que éstas se desarrollan. Si las tecnologías de la información y la comunicación (TIC) cambian tan rápidamente, en cuestión de meses los objetos y cuestiones relativas a éstas pueden quedar desfasados, ¿cómo es posible un pensamiento crítico sobre algo que cambia tan veloz y constantemente?¿qué ética aplicar a situaciones que no se mantienen en el tiempo?¿se puede aplicar una ética clásica a estas cuestiones? Estas dudas no tienen fácil respuesta, "no sólo por los embrollos conceptuales, sino también porque la moral general, los valores sociales y las normas no están claros con respecto a los detalles puestos en duda por la tecnología informática" (Johnson, 1996, p. 24).

1.1. La tradición ética frente a las cuestiones planteadas por las tecnologías digitales

Uno de los primeros objetos de estudio que se planteará la ética informática es saber si está tratando con objetos ya conocidos, las nociones clásicas de bueno o malo, justicia, intimidad, privacidad, propiedad, etc., o si, por el contrario, las tecnologías digitales traen consigo nuevos temas de estudio, problemas que la ética clásica no analiza o ni tan siquiera tiene en consideración. Como afirma Eduardo de Bustos,

> Las TIC no sólo transforman el acceso a la información, la producción de conocimiento y la vida social, sino que también, a consecuencia de ello, abren nuevos caminos de reflexión ética, fuerzan a la consideración analítica y crítica de nuevos desarrollos tecnológicos, de su impacto en la producción y distribución del conocimiento, y sobre la aparición de nuevos ámbitos de acciones y comportamientos éticos.
>
> (De Bustos, 2006, p. 47)

Este debate, que se ha convenido en llamar la cuestión de la singularidad de la ética informática, está todavía por resolver, pero en el seno de la propia cuestión se ha desarrollado un cambio fundamental. En los primeros momentos del debate la cuestión radicaba en saber si los ordenadores traían consigo nuevas cuestiones que pudieran abarcarse desde las teorías y posturas éticas tradicionales. En este sentido, la centralidad del discurso giraba en torno a las máquinas e instrumentos. Más tarde se introdujo la cuestión de la ética de la información en sí misma,

> Es decir, la presunta singularidad de la infoética, frente a la más antigua ética de los computadores o compuética, reside en que tiene como objeto una realidad no reducible, al menos desde el punto de vista moral, a una realidad material.
> (De Bustos, 2006, p. 48)

Siguiendo la reflexión realizada por Tavani (2002) se pueden encontrar dos posturas a la hora de abordar esta singularidad de la ética informática, que podrían denominarse tradicionalista y singularista. La primera afirmaría que las TIC no traen consigo nuevos problemas éticos. El modo de analizar los problemas éticos que puedan surgir de las TIC deben resolverse del mismo modo que se resuelven, por analogía, otras cuestiones. Éstas no modifican el seno de la ética sino que plantean la necesidad de abordarlas desde puntos de vista nuevos. Los singularistas, por su parte, afirmarían la radical novedad de las cuestiones éticas, que necesitan de nuevos marcos teóricos y métodos de aplicación diferentes a los tradicionales. Dentro de éstos se pueden encontrar dos líneas de actuación: aquellos que consideran que las TIC traen nuevos problemas que deben integrarse en las teorías tradicionales; y aquellos que afirman la necesidad de todo un nuevo marco teórico para su análisis.

Que la ética informática trae consigo nuevos problemas éticos es la opinión de Walter Maner que a finales de la década de los setenta proponía el nombre de "computer ethics" para una nueva rama de la ética que se dedicara a estudiar los problemas éticos generados por el uso de la tecnología. Pionero en el estudio de la ética informática y en la introducción de esta disciplina en el mundo académico, publica en 1978 *Starter Kit on Teaching Computer Ethics.*

En 1985 Deborah G. Johnson publica lo que será el primer manual de ética informática para estudiantes, *Computer Ethics.* Considerado el primer manual o libro de texto utilizado durante décadas por los estudiantes de esta nueva disciplina y referente fundacional de lo que ya se iba

gestando desde hacía cuarenta años. Si bien la tecnología ha avanzado a tal velocidad que las cuestiones que plantea Johnson en su libro se quedan insuficientes para resolver la cantidad de problemas que plantean actualmente las TIC a la ética, la obra trata aspectos que todavía hoy están por resolver y analiza una serie de ejemplos que ponen de manifiesto la dificultad de dar una única respuesta válida para las cuestiones que impone la ética informática, como son la privacidad, la propiedad intelectual y de software o el hackerismo, entre otros.

A diferencia de Maner, Johnson considera que la ética informática supone un planteamiento nuevo a problemas tradicionales, que de base no han cambiado con las TIC, "propongo que pensemos en los problemas éticos relacionados con los ordenadores como una nueva especie de viejos problemas éticos" (Jonhson, 1996, p. 26). La intimidad, privacidad, propiedad intelectual, etc., no son temas nuevos. El matiz está en la medida en que esa intimidad, privacidad y propiedad intelectual puede ser respetada, quebrantada, utilizada, etc., con o por el uso de las nuevas tecnologías. Ahora bien, Johnson es consciente de que todas estas cuestiones adquieren una dimensión extraordinaria cuando se plantean dentro de las TIC y la ética informática y que aunque se traten viejos problemas éstos han sufrido un cambio significativo en la medida en que se han introducido nuevos elementos de análisis así como puntos de vista. Estos viejos problemas adquieren importancia capital con las tecnologías digitales, debido en parte a que el alcance de los mismos se ha ramificado hacia aspectos donde antes no tocaban o simplemente no existían.

Los problemas a los que se enfrenta la ética informática no son para la autora, de base, problemas nuevos sino, en todo caso, cuestiones viejas que deben ser tratadas de un modo novedoso por su dimensión. Así, las definiciones y cuestiones que plantea la ética informática no se distinguen mucho de una ética tradicional, pues ésta "resulta ser el estudio de los seres humanos y la sociedad, así como nuestras metas y nuestros valores, nuestras normas de comportamiento, las maneras en las que nos organizamos y conferimos derechos y responsabilidades" (Jonhson, 1996, pp. 20-21).

La cuestión de la propiedad intelectual, por ejemplo, se amplía hacia múltiples frentes que ponen de manifiesto, según Johnson, estos nuevos campos de estudio para la ética, como son la propiedad del software o de algoritmos matemáticos, entre otros. El Pagerank, el algoritmo utilizado por el motor de búsqueda Google para ordenar, clasificar y presentar la información al usuario es uno de los secretos mejor guardados de la empresa y está protegido bajo el derecho a la propiedad intelectual.

Esto se debe, principalmente, a que esta clasificación, ordenación y presentación del motor que le otorga el algoritmo le convierten en el mejor motor de búsqueda del mercado.

> PageRank is a Web page ranking technique that has been a fundamental ingredient in the development and success of the Google search engine […] Today, the Web is a huge, dynamic, self-organized, and hyperlinked data source, very different from traditional document collections which are nonlinked, mostly static, centrally collected and organized by specialists. In 1998, Sergey Brin and Larry Page revolutionised the field of Web information retrieval […] The method was implemented in the famous PageRank algorithm and both the traditional content score and the new importance score were efficiently combined in a new search engine named Google.
> (Franceschet, 2010, p. 1)

Ahora bien, un algoritmo no deja de ser una serie de instrucciones, de pasos, que de seguirse en el orden adecuado siempre darán el mismo resultado para todos los casos. Esto es, una secuencia lógica matemática que permite llevar a resultados siempre iguales y predecibles. Pura matemática. Este ejemplo pone de manifiesto el hecho que la tecnología plantea como una nueva cuestión el tener que pensar éticamente la posibilidad de que las matemáticas puedan ser propiedad de alguien, esto es, patentadas.

Algo similar ocurre con el software. El software es un conjunto de herramientas que permiten al ordenador (hardware) realizar tareas determinadas. Dicho de otro modo, es el conjunto de componentes lógicos (de ahí su traducción como soporte lógico) de un ordenador. Existen diversos tipos de programas, tales como los software de sistema, los de programación o los de aplicación. Entre los primeros se encuentran los sistemas operativos, un conjunto de programas que permite al hardware funcionar como un ordenador y al usuario le ofrece la posibilidad de realizar tareas con él. Entre los sistemas de programación están los compiladores, encargados de traducir a un lenguaje entendible para el usuario todo aquello que computa la máquina, es aquello que traduce los ceros y unos del lenguaje binario a un lenguaje comprensible para un humano. Un software de aplicación es un programa o conjunto de programas que permiten al usuario realizar tareas específicas. Las aplicaciones utilizadas en los móviles y tabletas para leer, jugar, hacer ejercicio, observar las estrellas y un largo etcétera están dentro de este tipo de software.

El software y su propiedad están en el punto de mira de la ética informática. Mientras unos opinan que se está privatizando un conjunto de reglas y que como tal no deberían poder ser propiedad de nadie, como podrían ser los defensores del software libre (Lawrence Lessig sería su defensor más conocido), otros afirman que la unión de ese conjunto de reglas establecidas en un orden concreto debe ser considerado como una creación individual y como tal puede acogerse al derecho de propiedad individual y su correspondiente pago al creador por su uso. Google y su PageRank sería un claro ejemplo de defensa de esta postura. Tanto los algoritmos como el software son ahora centrales a la hora de abordar la propiedad intelectual, enteramente nuevos y necesariamente vinculados al desarrollo de la tecnología y la computación.

Otra tarea novedosa para la ética es el intercambio de información a gran escala. La era digital ha supuesto un movimiento de información como nunca se había conocido. En épocas pasadas el paso del mito al logos o de la tradición oral a la escrita había supuesto ya la preocupación a este respecto y todas las épocas con cambios tecnológicos han tenido sus críticos que veían con miedo esos avances, obstinados en creer que la cultura y el conocimiento estaban viviendo sus últimos momentos debido a esas nuevas formas de transmisión de saber.

Ya en Platón se encuentra esta preocupación por los cambios, si se quiere tecnológicos, que pueden desembocar en un menosprecio de las cualidades humanas. Así lo expresaba en el *Fedro* en boca de Sócrates a propósito de la escritura, cuando éste le cuenta a aquél una tradición de los antiguos (en referencia a los egipcios):

> Padre de la escritura [le dice el rey Tamus a Teut, dios inventor de avances científicos] y entusiasmado con tu invención, le atribuyes todo lo contrario de sus efectos verdaderos. Ella [la escritura] sólo producirá el olvido en las almas de los que la conozcan, haciéndoles despreciar la memoria; confiados en este auxilio extraño abandonarán a caracteres materiales el cuidado de conservar los recuerdos, cuyo rastro habrá perdido su espíritu.
> (Platón, Fedro, 274c-277a).

En la era digital poca información queda que no sea intercambiada o intercambiable. Esto ha supuesto un gran avance respecto a épocas pasadas, cuando la información era custodiada por unos pocos privilegiados que administraban el saber humano. Pero esta diseminación del conocimiento

ha traído consigo también sus consecuencias. El problema no surge ahora del acceso a esa información sino bien al contrario del exceso de accesibilidad. Todo aquello que está en la red es compartible, incluso aquello que uno no desearía compartir. Se podría decir, incluso, que en la red toda información es información compartida.

Esto supone un problema viejo pero con una dimensión nueva. El intercambio de información adquiere una importancia capital en el ciberespacio, pues todo movimiento en la red es información y como tal es accesible para alguien. Cuando un internauta hace uso de la red deja una huella digital en todo el recorrido y tiempo que esté en el ciberespacio. Esa impronta supone a su vez una fuente de información sobre las preferencias del usuario, intereses, costumbres, hábitos, aficiones, situación económica y laboral, etc. La posesión de esa información se traduce en una fuente de ingresos para quién sepa hacer uso de ella. Ese intercambio de información, entendido como huella digital es uno de los retos de la ética informática y en concreto de la ciberética. Las preguntas que se desprenden en términos éticos son ¿en qué medida la huella digital es inherente o necesaria en la red? Si es inevitable esa huella ¿es propiedad privada de la persona que la imprime? Si es necesaria y es propiedad privada de las personas ¿debería haber algún tipo de compensación económica al propietario de la huella?

Algunas de estas preguntas han intentado ser contestadas. Luciano Floridi, por ejemplo, afirma que en la medida en que actualmente todo es información, ésta debe ser entendida y tratada como un agente moral.

> IE's (ética de la información) claim consists of two these. The first thesis states that information objects qua information objects can be moral agents [...] The second thesis states that information objects qua information objects can have an intrinsec moral value.
> (Floridi, 2002, p. 11)

Jaron Lanier (2014) propone una acción radical ante el uso de esa información de los cibernautas por parte de las productores-usuarios. Para él, los cibernautas, y su información, no son tratados como realmente deberían serlo. En su opinión, los ordenadores, Internet y el ciberespacio en general no significarían nada sin la fuente de información que suponen los individuos que los usan y habitan, por lo tanto éstos deberían, al menos, recibir una compensación económica por ello.

> Si esa información permite que un robot simule ser capaz de mantener una conversación natural, o que una campaña política dirija su mensaje a determinados votantes, la persona de la que se obtiene debería recibir una compensación económica por su utilización. A fin de cuentas, de no ser por ella, los datos no existirían.
> (Lanier, 2014, p. 39)

Estas dos propuestas difieren entre sí pero comparten la idea de abordar la cuestión del uso de la información de un modo novedoso para la ética. Ambas ponen de manifiesto la necesidad de pensar los problemas éticos derivados de las tecnologías digitales, primero desde un punto de vista moral, y segundo desde perspectivas que pueden resultar ajenas a la ética tradicional pero que no pueden ser descartadas por el simple hecho de no haber sido pensadas hasta este momento.

En octubre de 1985 la revista *Metaphilosophy* publica un número especial sobre ética informática. En él se presenta un artículo de James Moor bajo el título *What is Computer Ethics?* Moor propone una definición de la ética informática mostrando los motivos por los que los ordenadores y la informática hacen surgir nuevos problemas para la ética y en mayor medida que otro tipo de tecnología. Para Moor la ética informática "is the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology" (Moor, 1985, p. 262). La ética informática debe encargarse de proponer normas de comportamiento en el uso de la tecnología, ya que "a typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used" (Moor, 1985, p. 266).

Moor pone de manifiesto el vacío legal o normativo que padece el uso de las TIC. Este vacío normativo sigue siendo, a pesar de los avances por superarlo, casi veinticinco años después de la publicación del artículo de Moor, objeto de discusión en la ética informática y por ende en la ciberética en la actualidad. Quién debe decidir las normas, bajo qué criterios, qué normas deben aplicarse o quién debe obedecerlas son algunas de las preguntas para las cuales se siguen buscando respuestas.

Lo revolucionario y novedoso de la ética informática y en concreto del uso generalizado de los ordenadores se debe, para Moor, a la maleabiliad lógica de los mismos. La dificultad de responder a las preguntas anteriores deriva también, en parte, de esa maleabilidad.

> The essence of the Computer Revolution is found in the nature of a computer itself. What is revolutionary about computers is logical malleability. Computers are logically malleable in that they can be shaped and molded to do any activity that can be characterized in terms of inputs, outputs, and connecting logical operations..."I think logical malleability explains the already widespread application of computers and hints at the enormous impact computers are destined to have. Understanding the logical malleability of computers is essential to understanding the power of the developing technological revolution. Understanding logical malleability is also important in setting policies for the use of computers. Other ways of conceiving computers serve less well as a basis for formulating and justifying policies for action. (Moor, 1985, p. 269).

Junto con la idea de maleabilidad lógica Moor añade a su teoría lo que él llama valores humanos fundamentales (*core human values*). Vida, salud, felicidad, seguridad, conocimiento, etc., son aspectos a tener en cuenta a la hora de analizar éticamente la relación de los seres humanos y las tecnologías.

> The combined notions of human life, happiness, and autonomy may not be far from what Aristotle meant by “human flourishing”. Thus, from an ethical point of view we seek computing policies that al least protect, if not promote, human flourishing.
> (Moor, 1999, p. 65)

El consecuencialismo, limitado por la justicia, combinado con una normatividad basada en la idea de "imparcialidad moral" y la "venda de la justicia" de Gert (1998) son para Moor la vía que permite resolver los problemas relacionados con las TIC. Problemas que pueden perjudicar, de algún modo, esos valores humanos.

> If the blindfold of justice is applied to computing policies, some policies will be regarded as unjust by all rational, impartial people, some policies will be regarded as just by all rational, impartial people, and some will be in dispute. This approach is good enough to provide just constraints on consequentialism .
> (Moor, 1999, p. 67)

Así, todas las propuestas deben pasar por un examen sobre la imparcialidad y escoger entre todas ellas aquellas que sean más justas.

> We first require that all computing policies pass the impartiality test. Clearly, our computing policies should not be among those that every rational, impartial person would regard as unjust. Then we can further select policies by looking at their beneficial consequences. We are not ethically required to select policies with the best possible outcomes, but we can assess the merits of the various policies using consequentialist considerations and we may select very good ones from those that are just.
> (Moor, 1999, p. 68)

1.2. El establecimiento de la ciberética en la academia

En la década de los noventa la ética informática es ya una realidad en las universidades. Simposios, conferencias y cursos son impartidos en diversas y numerosas facultades. Una de estas universidades es De Montfort University, en Leicester. Esta universidad crea el Centro de Computación y Responsabilidad Social o CCSR, en sus siglas en inglés. Entre sus objetivos está, según afirman en su página web "to undertake research and provide teaching, consultancy and advice to individuals, communities, organisations and governments at local, national and international levels on the actual and potential impacts of computing and related technologies on society and its citizens" [4].

Otras universidades, como Oxford University se han ido uniendo a crear programas dedicados al estudio del ciberepacio y en concreto de Internet. Esta universidad creaba en 2001 el Oxford Internet Institute bajo el lema *Understanding life online.* El instituto cuenta con programas de master y doctorados, relacionados con ciencias sociales en Internet, comunicación en línea o filosofía de la información.

En 1995 el CCSR organiza el ETHICOMP, un congreso o ciclo de conferencias donde se tratan cuestiones éticas y sociales relacionadas con las TIC con el objetivo de "to provide an inclusive

[4] http://www.dmu.ac.uk/research/research-faculties-and-institutes/technology/centre-for-computing-and-social-responsibility/ccsr-home.aspx

forum for discussing the ethical and social issues associated with the development and application of Information and Communication Technology"[5].

En este congreso Krystina Górniak-Kocikowska presenta una ponencia bajo el título *The Computer Revolution and the Problem of Global Ethics*. En ella anuncia una tesis que actualmente resulta vaticinadora, a saber, que las nuevas tecnologías suponen una revolución y que sus cuestiones tienen un alcance global. La ética informática, resume, a diferencia de las éticas tradicionales basadas en las costumbres y tradiciones europeas, esto es, en un punto de vista determinado por el contexto cultural de la sociedad en la que se desarrollan, lleva consigo una ética global adecuada para cualquier cultura o sociedad en la que haya tecnologías informáticas. "[...] the rules of computer ethics should be respected by the majority (or all) of the human inhabitants of the Earth [...] In other words, computer ethics will become universal, it will be a global ethic" (Górniak-Kocikoswka, 1996, p. 187).

Así pues, la revolución informática, que supone una revolución ética, conlleva un cambio de paradigma para la ética. Hasta ahora, incapaz de superar los localismos, la ética no podía hacer frente al relativismo cultural y a las críticas derivadas de éste, en la medida en que las propuestas éticas podían no ser compartidas por una parte de la población, una sociedad o un país, ya que sus tradiciones culturales no estaban fundamentadas en las mismas creencias o hábitos que aquellas de las que nacían las propuestas éticas.

La propuesta de Górniak-Kocikoswka se basa en la idea que la ética informática llevará (en el futuro de 1995) a una ética global. La naturaleza misma de esta revolución informática es su carácter global. "It will be global in a spatial sense, since it will encompass the entire globe. It will also be global in the sense that it will address the totality of human actions and relations" (Górniak-Kocikoswka, 1996, p. 179).

Una ética global como la que propone la autora debe llevar consigo necesariamente una comunidad, también global, que acepte y participe de esos valores y normas de conducta. Por esta razón, diez años más tarde, Górniak-Kocikoswka publica un artículo bajo el título *"From Computer Ethics to the Ethics of Global ICT Society*". En él aprovecha para confirmar lo que ya había supuesto en

[5] http://www.dmu.ac.uk/research/research-faculties-and-institutes/technology/centre-for-computing-and-social-responsibility/ethicomp-series.aspx

1995, a saber, que la revolución de los ordenadores supondría la necesidad de una ética global y una comunidad que la aceptara.

En primer lugar, para evidenciar cómo los ordenadores y las TIC han alcanzado todos los aspectos de la vida diaria. Hace un repaso a los nombres que ha ido tomando la revolución de los ordenadores. Lejos de ser una simple cuestión de conceptualización, las diversas acepciones que han tenido las tecnologías digitales son un claro ejemplo de cómo han ido tomando terreno esas tecnologías en la vida humana.

> Firstly, I would like to focus on the significance of the changes in the names given to the technology we called, among others, computer technology,digital technology, information technology, and information and communication technology. This evolution reflects also the changes in the perception of a computer.
> (Górniak-Kocikoswka, 2007, p. 2)

Lo que en un primer momento se llamó "tecnología computacional", "tecnología digital", "tecnología informacional" o "tecnologías de la información y la comunicación" no tenía en cuenta el aspecto humano de esta nueva ciencia. Estas definiciones no expresaba ninguna humanidad y podían interpretarse como si los humanos no participaran de ellas. No había nada en los conceptos que hiciera pensar que éstos tenían que ver con los usuarios de esas tecnologías. Su definición sólo expresaba el hecho digital o computacional, esto es, tecnológico.

Con el avance de estas tecnologías también progresaba el alcance de las mismas. A medida que tomaban relevancia en los diversos aspectos de la vida diaria de las personas y se instalaban en ella como un nuevo espacio social se convino introducir el concepto de "era". Esta nueva acepción tiene como característica principal la inclusión de una temporalidad humana, introduce la idea de humanidad en la medida en que supone un hito para la misma, significa un cambio en la vida y en la cultura. Así, de la "era de los ordenadores" a la "era digital" y de ésta a la "era TIC". A pesar de esta introducción, estos conceptos, sin embargo, tienen todavía como eje central la tecnología misma como si los sujetos de esta era fueran las propias máquinas y los avances tecnológicos y los humanos un mero predicado.

Actualmente ya se habla de “sociedad basada en los ordenadores” o “sociedad TIC”. El aspecto central ahora es la comunidad de seres humanos, en torno a la cual se desarrollan las tecnologías.

> Interestingly enough, the terms describing core characteristics of our leading technology become progressively more inclusive. It seems that the more we are aware of how many areas of our lives are affected, or even controlled, by this technology, the more general, more inclusive its name.
> (Górniak-Kocikoswka, 2007, p. 2)

Esta sociedad se define ahora por el acceso a la información y a las comunicaciones. Esto supone a su vez un acceso al conocimiento, de ahí que también se llame “sociedad del conocimiento” o “sociedad del conocimiento y la información”. Esta información en la “aldea global”, que no se transmite y genera sola, sino con el apoyo de la tecnología y ésta con el apoyo de empresas e instituciones, ha supuesto así mismo un nuevo modelo económico, lo que se conoce como “economía del conocimiento”, donde la producción de riqueza está basada, en su mayoría, en la generación y gestión del conocimiento. Este conocimiento en las TIC es información.

Aunque se tienden a utilizar de forma indistinta los conceptos de sociedad del conocimiento y economía del conocimiento deben tenerse como diferentes, puntualiza la autora. Es necesaria una distinción entre ambos ya que es precisamente en esa diferencia donde radican las cuestiones éticas. Para hacer la aclaración se ayuda de la distinción de Joel Mokyr (2002) entre el saber “qué” del conocimiento, de carácter teórico e inclinado al concepto de sociedad del conocimiento y el saber “cómo” del conocimiento, éste prescriptivo e interesado en el concepto de economía del conocimiento. La ética, según la autora, estaría más preocupada por la sociedad que por la economía del conocimiento:

> It seems that scholars who are more interested in the theoretical, propositional knowledge are inclined to favor the idea of the knowledge society, whereas those involved with the prescriptive knowledge, favor the concept of knowledge economy. With regard to ethics it seems that there is a much greater interest in moral issues regarding knowledge society than it is in relation to knowledge economy; a quite understandable situation, albeit hardly a desirable one.
> (Górniak-Kocikoswka, 2007, p. 3)

Dicho de otro modo, la economía del conocimiento es el modelo que adopta la economía en la sociedad del conocimiento. El problema parece derivar, paradójicamente, en la falta de comunicación entre ambos conceptos. De ahí que la autora plantee la necesidad de crear un puente que permita la comunicación entre ambas sociedades y que sirva para resolver los problemas que puedan derivarse de esa segregación.

> In any case, it seems to be worth while to ask whether it would be possible to build a bridge between knowledge society and knowledge economy; and if so, what kind of ethical problems could be solved that way. ICT could be helpful here, since ICT, the universal technology, is used for the advancement of both propositional and prescriptive knowledge.
> (Górniak-Kocikoswka, 2007, p. 3)

Las TIC pueden ofrecer las herramientas necesarias para la creación de ese puente. En primer lugar porque responden tanto a la sociedad como a la economía del conocimiento. Promueven y desarrollan el conocimiento teórico y el prescriptivo. En segundo lugar porque el concepto mismo de TIC lleva en si la unión de la tecnología y la comunicación, lo que viene a ser la economía y la sociedad respectivamente.

Esta investigación bien podría entenderse como un intento de construcción de ese puente entre la economía del conocimiento y la sociedad del conocimiento. A través de un análisis consecuencialista de los objetivos y medios de esa economía del conocimiento, representada en este caso por Google Inc., hoy ya Alphabet Inc., y sus consecuencias en la sociedad del conocimiento, se pueden vislumbrar qué elementos actúan como destructores o constructores de ese posible puente entre ambos lados de las tecnologías digitales.

En definitiva, la ética informática en sus inicios se preocupa de sentar sus propias bases, el marco de actuación en el cual debe obrar. El debate entre nuevos-viejos problemas éticos, los límites de su alcance o sus bases teóricas son algunos de los temas que preocupan a los pioneros de esta disciplina. A medida que las tecnologías digitales avanzan y que éstas transformarán el modo en que los humanos se relacionan con ellas y entre sí, nuevas voces aparecen en la historia de la ciberética reclamando su lugar en ella.

No es una historia paralela y separada pero su perspectiva sí es diferente. Su análisis versa sobre la organización social que adquiere el ciberespacio y las relaciones sociales y personales que en él surgen. Organización social y relaciones sociales que desembocan por ende en lo que se puede denominar sociología del ciberespacio. Un par de ejemplos serán suficientes para mostrar cómo la ciberética se vuelve una rama del pensamiento interdisciplinar, donde cada ciencia puede y tiene algo que decir sobre la importancia de pensar sobre estos cambios que la tecnología de la información está trayendo consigo. Esta sociología de la red se verá más adelante (sección 1.4.) pero antes es necesario señalar los primeros intentos de definir unas normas de conducta para la TIC y las tecnologías digitales.

1.3. Primeras aproximaciones a una definición de ciberética.

La Stanford Encyclopedia of Philosophy define la ciberética como las cuestiones relativas a la ética informática relacionadas con Internet[6]. Entre otras definiciones de ética informática que implican la aplicación de teorías éticas occidentales a casos que involucran a los ordenadores y las redes informáticas, "Computer ethics also has been used to refer to a kind of professional ethics in wich computer professionals apply codes of ethics and standards of good practice within their profession" [7]. Se debe, por lo tanto, poder aplicar esos códigos éticos a esa parte de la ética informática que se dedica a cuestiones relativas al ciberespacio.

La ética informática tiene sus propios agentes. Ingenieros, diseñadores, programadores o técnicos, todos ellos tienen, dentro de sus disciplinas, códigos de conducta que les guían a la hora de realizar sus tareas. De este modo se pueden encontrar ejemplos de intentos de marcar unas directrices de carácter ético para el diseño de artefactos tecnológicos.

Ya en 1992 el Consejo de la Association for Computing Machinery (ACM) aprobaba un código ético basado en 24 imperativos que pudieran servir "como base para tomar decisiones éticamente con respecto a la conducta del trabajo profesional. Secundariamente, pueden servir como base para juzgar una demanda formal relacionada con la violación de las normas éticas de una profesión" (Johnson, 1996, p. 214). Este código se presenta dividido en cuatro apartados: ocho imperativos morales generales; ocho responsabilidades profesionales específicas; seis imperativos de liderazgo; y dos cumplimientos del código.

---

[6] http://plato.stanford.edu/entries/ethics-computer/

[7] idem.

A continuación se señalan los imperativos morales generales, pues son éstos los que permiten una aproximación a los conceptos de la ética informática que se incluyen, con más frecuencia, en el análisis del ciberespacio[8]. Estos conceptos, que se adelantan aquí, son: la privacidad e intimidad; la propiedad intelectual; la responsabilidad profesional; los derechos de software; el acceso y la autonomía; y la vigilancia y censura. Los imperativos morales generales que rubrica cada miembro de la ACM son:

1. Contribuiré al bienestar humano y de la humanidad.
2. Evitaré perjudicar a otros.
3. Seré honesto y fidedigno.
4. Respetaré los derechos de propiedad incluyendo los derechos de autor y las patentes.
5. Daré el debido crédito a la propiedad intelectual.
6. Respetaré la intimidad de otros.
7. Respetaré la confidencialidad.

Por bienestar humano y de la humanidad se entiende el respeto por los derechos humanos y la diversidad cultural así como un esfuerzo por crear un ambiente social y natural seguro. Evitar perjudicar a los otros significa que la tecnología debe minimizar el daño que ésta pueda causar a las personas y a la sociedad en general. Dentro de este daño se incluyen las acciones directamente perjudiciales pero también las acciones que de un modo indirecto puedan causar algún perjuicio a los individuos. Esto es, la pérdida de información, la inclusión de virus informáticos o la pérdida de recursos humanos por negligencia. Pero también se incluye la falsedad u omisión de información a los usuarios, donde el profesional o profesionales involucrados serán los responsables directos del daño causado.

No causar daño implica ser honesto y fidedigno con la tarea que se realiza. Honesto a la hora de exponer las implicaciones del diseño tecnológico, no ocultar información que sea relevante para el uso del sistema que se está realizando y supone la obligación de dar cualquier tipo de información relevante sobre el artefacto o producto. Ser justo y sin discriminación supone la asunción de que toda persona, sin excepción, tenga derecho al uso de la tecnología, la información y los recursos

[8] Para una lectura completa de este código ético véase https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct

informáticos disponibles. Ahora bien, estos recursos informáticos no deben ser utilizados para llevar a cabo acciones que vayan en contra de cualquiera de los puntos expuestos en este código ético.

Por otra parte se han de respetar los derechos de propiedad intelectual y las patentes. El hecho de que un programa no esté protegido con derechos de propiedad intelectual no debe ser motivo para hacer un mal uso o utilizarlo de modo que pueda dañar de algún modo, pues en este caso se estarían vulnerando otros puntos de este código. Así mismo, el hecho que una invención no esté protegida con derechos de propiedad intelectual no significa que pueda ser reclamada por una persona o institución como propia. De ahí que se deba dar crédito a la propiedad intelectual y no apropiarse de invenciones ajenas.

Por último, debido a la posibilidad que ofrece la tecnología de recabar información personal de individuos o instituciones, los profesionales deberán proteger y mantener la intimidad de las personas. Entre sus misiones estará la de diseñar y construir herramientas que permitan la protección de esa intimidad. Así mismo se exige que el almacenamiento de la información personal sea la estrictamente necesaria y por un tiempo determinado y que exista la posibilidad real de que los individuos puedan acceder, editar y corregir la información personal que consideren necesaria u oportuna. Este aspecto lleva al último punto consignado de respetar la confidencialidad de la información de la que se dispone, salvo en el caso en que la legalidad lo requiera.

Estas aclaraciones se encuentran incluidas en el propio código ético de la AMC. Aquí han sido resumidas pero se han mantenido las ideas generales. Como se ha hecho notar más arriba, son indicaciones para el diseño y creación de herramientas informáticas. Aunque Internet ocupa un lugar muy amplio en las tecnologías digitales y bien podría considerarse un lugar aparte dentro de éstas, lo cierto es que no deja de ser una tecnología digital más, por lo que la aplicación de estos compromisos al ciberespacio, y en concreto a Internet, está justificada y puede servir de guía a la hora de pensar un código ético que sirva también para este nuevo espacio social.

Otra organización donde se puede encontrar un interés por la eticidad de las tecnologías digitales es la International Federation for Information Processing. Constituida en 1960 tras el primer Congreso Mundial de Informática en 1959, forma parte de los órganos consultivos de la UNESCO sobre temas relacionados con la informática y las telecomunicaciones. Si bien no contiene, como en la AMC, un estatuto sobre la buena praxis informática, ha elaborado varios documentos donde se

indica la necesidad de una ética para las tecnologías digitales, así como los motivos por los que esto es necesario y la conveniencia de una ética aplicada a este campo. En uno de esos documentos[9] reclaman una gobernanza ética para Internet. *"We need IT ethics because:*

- *IT is a powerful and constantly evolving tool,*
- *IT permeates all aspects of our lives,*
- *IT dependency creates vulnerability on a large scale,*
- *It evolution and usage outsrips the formulation and implementation of policy and legal instruments".*

Entre todos los aspectos que considera la organización que deben tener un contenido ético están:

- *equity in the right access;*
- *questions linked to the respect of the dignity of the person;*
- *justice and social exclusion;*
- *respect for the interests and the rights of the persons;*
- *free speech/censorship;*
- *quality of life;*
- *right to information;*
- *personal qualities;*
- *non-abuse of power;*
- *respect for cultural differences;*
- *freedom of chice in the user or non-user of the Internet;*
- *grounding "virtual" life in the physical realm[10].*

En 1992, el Computer Ethics Institute creaba los diez mandamientos para la ética informática. Del mismo modo que los anteriores, sus propuestas tiene como objetivo hacer del ciberespacio un lugar seguro y justo para todos sus habitantes. Estos mandamientos se presentan así:

1. *Thou shalt not use a computer to harm other people.*

---

[9] Cameron, J., Clarke, R, Davies, S., Jackson, A., Prentice, M. y Regan, B. (1992) Ethics, Vulnerability and Information Technology. *Ethics of Computing: Codes, Spaces for Discussion and Law 2,* (2), 344-350

[10] https://staff.info.unamur.be/jbl/IFIP/Ethics_and_Internet_Governance.pdf

2. *Thou shalt not interfere with other people's computer work.*
3. *Thou shalt not snoop around in other people's computer files.*
4. *Thou shalt not use a computer to steal.*
5. *Thou shalt not use a computer to bear false witness.*
6. *Thou shalt not copy or use proprietary software for which you have not paid.*
7. *Thou shalt not use other people's computer resources without authorization or proper compensation.*
8. *Thou shalt not appropriate other people's intellectual output.*
9. *Thou shalt think about the social consequences of the program you are writing or the system you are designing.*
10. *Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.*

Desde otro punto de vista, la Internet Architecture Board definía en 1989 aquello que se consideraba poco ético dentro de la ética informática. Esta perspectiva no desea tanto marcar los límites poniendo reglas sino actuar de modo que se eviten unas consecuencias concretas. Así, una acción se considerará inapropiada o poco ética cuando:

1. *Seeks to gain unauthorized access to the resources of the Internet.*
2. *Disrupts the intended use the Internet.*
3. *Wastes resources (people, capacity, computer) through such actions.*
4. *Destroys the integrity of computer-based information, or*
5. *Compromise the privacy users*[11]

Como puede observarse, las exigencias o preocupaciones fundamentales para estas organizaciones no distan mucho entre sí. Sus objetivos se centran en el respeto a los derechos fundamentales de las personas dentro del ciberespacio e Internet. El problema radica, como en el mundo real o no digital, en la dificultad de llevar estos derechos a la práctica. El modo en que se construye y habita el ciberespacio es tan sólo un reflejo de cómo se vive en el mundo físico y por tanto, los defectos humanos son también defectos en el mundo digital.

---

[11] https://tools.ietf.org/html/rfc1087

Estas son sólo un ejemplo de las organizaciones que trabajan por incluir aspectos éticos en el ciberespacio. Pero no son las únicas. La Electronic Frontier Foundation trabaja por la realidad de la libertad de expresión en Internet, el uso justo y equilibrado de la propiedad intelectual, el apoyo a la innovación tecnológica, contra la violación de la privacidad, apoyando y fortaleciendo los derechos de los consumidores en Internet y por una transparencia por parte de los gobiernos sobre el uso que hacen de las tecnologías digitales[12]. Otras organizaciones como el International Centre for Information Ethics[13] o la Computer Professionals for Social Responsibility[14] trabajan por la unión de profesionales tecnológicos que puedan examinar y determinar el uso de las tecnologías digitales para la defensa de los derechos humanos y las libertades en el ciberespacio.

Todas ellas comparten los mismos objetivos y preocupaciones. Unas lo hacen desde la propia comunidad científica, productora de tecnología y otras desde las instituciones académicas o desde la población civil. Pero todas ellas comparten la idea de que existe una necesidad de pensar el ciberespacio como un lugar real donde existe una comunidad de ciberciudadanos que necesita de una gobernabilidad lo más justa y democrática posible para todos los miembros de la misma.

Por otra parte todas ellas tienen en común, como se ha mencionado más arriba, unas preocupaciones concretas que pueden resumirse en: una preocupación por la privacidad e intimidad de los cibernautas incluyendo la información que de éstos se genera, mantiene y se utiliza en la red; la propiedad intelectual, no sólo de los creadores y productores de herramientas y servicios del ciberespacio sino también de la propiedad intelectual de los mismos usuarios como creadores de contenidos; la responsabilidad profesional de los arquitectos de la red, de los usuarios-productores de Internet y de todas las personas y organizaciones encargadas de la gestión del ciberespacio; los derechos de software, su adecuación o no a las necesidades de las empresas y los consumidores; el acceso a Internet y por tanto a una información global; y por último la regulación de la vigilancia de los cibernautas y la censura de contenidos. Evidentemente el orden de exposición de estas preocupaciones no responde a cuestiones jerárquicas y cada elemento es esencial para todas las organizaciones mencionadas y para la ciberética en general.

---

[12] https://www.eff.org/es/about

[13] http://icie.zkm.de/

[14] http://cpsr.org/

1. 4. Sociología de la red

1.4.1. Sociedad red

Uno de los autores que ha desarrollado en profundidad el tema de la sociología de Internet es el doctor Manuel Castells. Desde sus primeros intereses en urbanismo, Castells ha aportado a los estudios sobre las TIC todo un corpus teórico encaminado a la conceptualización y demarcación sociológicas de esta "era de la información". Entre sus muchas aportaciones en este campo algunas son especialmente interesantes para la contextualización de esta investigación. Sus ideas se podrían condensar en el supuesto que: actualmente se vive en una era de la información, que no sociedad de la información; desarrollada, en parte, por un cultura hacker; basada en el informacionalismo; y creadora de una sociedad red.

Destaca en primer lugar la negación por parte de Castells del uso de conceptos como sociedad del conocimiento o sociedad de la información. Esto se debe a que afirmar que la sociedad actual contiene más conocimiento o información que las pasadas supone por un lado un etnocentrismo científico y por otro lado un evolucionismo antropológico. Etnocentrismo porque supone la supremacía de la revolución tecnológica capitalista como modelo y guía de todas las sociedades actuales. Evolucionismo antropológico porque considerar la sociedad actual como sociedad del conocimiento o de la información presupone una sociedad basada en estadios superables por los nuevos avances tecnológicos estando ahora en el último y mejor de los momentos de la sociedad, añadiendo a la sociedad actual un juicio de valor difícilmente comprobable.

> El conocimiento y la información han sido esenciales en muchas de las sociedades históricamente conocidas, sino en todas. Hubo sin duda diferentes formas de conocimiento en muchos casos, pero el conocimiento, incluido el conocimiento científico, es siempre históricamente relativo.
> (Castells, en Himmanen, 2002, p. 109)

La era de la información está basada en un nuevo paradigma denominado *informacionalismo*. Lo que distingue a esta época histórica no es la cantidad de información que genera sino la capacidad de procesar esa información y la posibilidad de generar conocimiento con ese procesamiento[15]. Este nuevo paradigma se sustenta sobre la base de tres rasgos principales y distintivos, a saber, 1) la

[15] Esta generación y procesamiento de información será fundamental para entender las TIC y sus consecuencias éticas como afirma, entre otros, Helena Nissenbaum y que será tratado en el capítulo 4.

capacidad autónoma de ampliación de información de estas tecnologías, 2) su posibilidad recombinatoria y 3) su posibilidad distributiva.

Estas características del informacionalismo han sido el resultado de dos campos tecnológicos, a menudo tenidos como independientes: la microelectrónica y la ingeniería genética. De la microelectrónica forman parte los ordenadores, los microchips o las conexiones electrónicas. El software, fundamental para el procesamiento de la información, es dependiente de los circuitos para realizar su función. Esto ha permitido el desarrollo de una tecnología capaz de retroalimentarse, de generar información de manera autónoma y expandirse de un modo independiente al quehacer humano. Este es un salto cuantitativo exclusivo de la era de la información.

La capacidad recombinatoria de las tecnologías digitales es la base del funcionamiento de Internet, el hipertexto. Internet se basa hoy en la posibilidad de enlazar un objeto con otro desde un sitio a otro y la posibilidad de recombinar ambos puntos.

> El valor añadido de Internet en relación con otros medios de comunicación en su capacidad para recombinar productos y procesos de información en determinado tiempo, creando un nuevo resultado que es inmediatamente procesado por la Red, en un proceso interminable de producción de información, comunicación y feedback en tiempo real o en un tiempo determinado.
> (Castells, 2001, p. 41)

La flexibilidad de la información y la comunicación es también parte fundamental de este paradigma. Esta flexibilidad abarca no solo los diversos modos de producción de información sino también de distribución, multiplicación, integración y multiplicación de puntos de comunicación.

En cuanto al segundo campo tecnológico que ha propiciado este nuevo paradigma, la ingeniería genética, debe tenerse como una tecnología de la información y la comunicación a la altura de la microelectrónica. Esto se debe fundamentalmente a que esta ingeniería se basa en la decodificación y reprogramación de información de la materia viva. Así mismo, sin el desarrollo de la electrónica digital esta ingeniería hubiera sido imposible o al menos se hubiera retrasado en el tiempo tanto como el desarrollo de una tecnología capaz de analizar el código de información vital ya que "Existe una convergencia teórica entre los dos campos tecnológicos alrededor del paradigma

analítico basado en las redes, complejidad, auto-organización y propiedades emergentes" (Castells, 2004, p. 39).

Esta era de la información basada en el informacionalismo ha dado lugar a la sociedad que Castells denomina "sociedad red". La estructura social de ésta debe entenderse como compuesta de redes, esto es, un conjunto de nodos enlazados por las tecnologías de la información y de la comunicación medidas por la microelectrónica. Como el informacionalismo, la estructura social de la sociedad red se define por su flexibilidad, su adaptabilidad y su capacidad de auto-reconfiguración:

> Por lo tanto, lo específico de nuestro mundo es la extensión y el aumento del cuerpo y la mente de los sujetos humanos en redes de interacción alimentadas por las tecnologías de la comunicación basadas en la microelectrónica y que operan mediante software. Estas tecnologías [...] convergen con las nuevas tecnologías de ingeniería genética capaces de reprogramar las redes de comunicación de la materia viva. Sobre esta base se está expandiendo la nueva estructura que constituye los cimientos de nuestra sociedad: la sociedad red.
> (Castells, 2004, p. 34)

Esta sociedad red, dependiente del informacionalismo, no debe tenerse como consecuencia de la tecnología, aunque ésta haya cimentado las bases para su desarrollo e instauración como sociedad dominante. Según Castells, la sociedad red se debe a factores históricos aleatorios y fortuitos aunque necesarios para su evolución. En primer lugar se debe a la crisis del industrialismo, que vio agotadas sus vías de supervivencia al ser incapaz de asimilar el cambio de productividad desde la producción de energía a la producción de conocimiento. Esta deficiencia suponía la necesidad de cambiar el modelo de producción y por tanto de transformar el capital humano de modo que hubiera una fuerza de trabajo capaz de llevar a cabo esa nueva productividad.

Así mismo la crisis del estatismo vino a reforzar esa transformación en una sociedad red. Los gobiernos y sus políticas, incapaces de hacer frente a los cambios en los modos de producción, basaron sus esfuerzos en recortes sociales y laborales, a modo de salvavidas a la hora de restablecer los beneficios empresariales. En Estados Unidos y Gran Bretaña esto se tradujo en la disminución del poder político de los sindicatos, la disminución de los impuestos a las clases ricas y empresarios, la liberalización de los mercados y el derrumbamiento de las políticas keynesianas que

habían dominado la economía en los años precedentes. En la Unión Soviética la ralentización del desarrollo tecnológico fue el desencadenante de su derrumbamiento militar y económico. Con esta caída soviética, los países del tercer mundo tuvieron que lanzarse al modelo capitalista occidental, quedando éste como el último modelo económico.

Por último, los movimientos culturas y sociales de la década de los sesenta y setenta, orientados hacia un afán de libertad supusieron un acontecimiento fundamental para el desarrollo de la tecnología, "la cultura de la libertad personal, poblaba las mentes de los inventores que configuraron la verdadera revolución tecnológica" (Castells, 2004, p. 48). Esa idea de libertad iba acompañada de un sentimiento de compartir, de que las creaciones debían ser para y por el bien común.

> Se desafió la tradición de la propiedad de la invención afirmando el derecho a la difusión gratuita de los protocolos de fuente de Internet o de los programas de software que constituían la mayor parte de las aplicaciones del nuevo mundo informático.
> (Castells, 2004, p. 48).

Los verdaderos avances tecnológicos no fueron realizados por las empresas privadas defensoras del derecho de propiedad intelectual sino por la cultura libertaria que se esparcía por las universidades donde se tenía presente la idea de progreso científico basado en la puesta en común y el trabajo colectivo en los descubrimientos.

1.4.2. Tercer entorno

Como Castells, Javier Echeverría ha tratado de dar forma social a las tecnologías digitales, creando un corpus teórico que sitúa a la sociedad dentro de los cambios tecnológicos vividos en las últimas décadas. Tanto Castells como Echeverría son considerados los introductores de los estudios digitales en los países de habla hispana. La sociedad red de la que habla Manuel Castells estaría enmarcada en lo que Echeverría denomina el tercer entorno. Este nuevo entorno se define principalmente por su carácter artificial.

El primer entorno se caracteriza por ser un medio esencialmente natural, donde el ser humano y la vida en general se habría adaptado, de múltiples formas, a este medio a través de la interacción. Las

matemáticas y los sentidos eran los aspectos fundamentales en el primer entorno. Las primeras en un sentido topológico y métrico. Topológico porque sitúa el cuerpo en un espacio y tiempo determinado. Métrico porque el cuerpo tiene una tridimensionalidad específica. Los segundos porque posibilitan la interacción del cuerpo con el medio, que permite la adaptación y transformación del medio que dará lugar al segundo entorno.

El segundo entorno es el llamado el entorno urbano. Éste ya no se caracteriza por su naturalidad sino por ser un entorno construido: cultural y social. No significa la desaparición del primer entorno pero sí su modificación. Una transformación que tiene como objetivo acoger a la diversidad humana.

> Así como el primer entorno se caracteriza por su capacidad para integrar una multitud de formas de vida animal y vegetal, el segundo entorno se distingue por su aptitud para el despliegue y expansión de diversas formas de vida humana.
> (Echeverría, 1999, p. 42)

En este entorno, el cuerpo se cubre de una sobrenaturaleza. La vestimenta, la política, la religión o la cultura forman parte de esa sobrenaturaleza que convierte al cuerpo en persona. Estas formas sociales y culturales, y por tanto artificiales, modifican el cuerpo en dos sentidos. De un modo exterior al ampliar las fronteras métricas, marcadas ahora por componentes artificiales pero también de un modo interior en la medida en que la persona participa mentalmente de todos estos atributos culturales.

El tercer entorno es en cambio un entorno artificial. Como tal, es un espacio siempre en construcción, en la medida en que cada nueva tecnología supone una modificación en éste. Echeverría trata sobre siete artefactos tecnológicos en los que se sustenta este entorno: el teléfono, la radio, la televisión, el dinero electrónico, las redes telemáticas, el multimedia y hipertexto. Antes del teléfono ya se habían dado otras invenciones tecnológicas pero este dispositivo supuso un cambio de perspectiva. Este salto,

> [...] es porque las redes telefónicas prefiguran la estructura de lo que aquí llamamos tercer entorno. En lugar de transmitir a través del aire, como sucede en el entorno

> natural y urbano, el sonido circula a través de un medio tecnológico, y por ello el nuevo medio de comunicación es ante todo artificial.
> (Echeverría, 1999, p. 51)

Internet es actualmente el elemento destacable de este entorno artificial, en la medida que condensa muchas de las acciones que pueden desarrollarse. Así, es un medio de comunicación mediante el cual los individuos se comunican entre sí de un modo muy evolucionado con el avance de las vídeollamadas. Es también un medio de información. No sólo por el hecho del acceso a medios informativos tradicionales sino por nuevas formas de acceso a la información como las redes sociales. Supone así mismo un medio mnemotécnico debido a su capacidad de almacenamiento. Por su capacidad de generar y almacenar información Internet es también un medio de producción y esto a su vez lo sitúa como medio de comercio e intercambio. Es un espacio donde se puede comprar y vender información pero también cualquier tipo de producto a través de tiendas y empresas en línea. Sin lugar a dudas Internet es también un medio de ocio y entretenimiento. No sólo en el sentido que abarca la televisión y radio, elementos de por sí cimientos del tercer entorno. La industria del ocio en Internet tiene un papel predominante en la economía digital. Cuando se habla de ocio y entretenimiento en Internet no debe pensarse exclusivamente en juegos. Dentro de este mercado deben tenerse las apuestas y juegos de azar; el turismo y la compra de viajes, hoteles, excursiones; la pornografía; la cultura, que engloba los conciertos, el teatro, el cine, la danza, entradas a museos; la restauración, etc.

Todas estas expresiones de Internet se fundamentan y condensan en una sola. Internet es sobre todo un medio de interacción humana. Toda acción realizada en la red, con independencia de la soledad o la compañía en la que se efectúe siempre tiene un componente de acción comunicativa. Siempre se hablará de un medio de comunicación creado por personas informando a personas, de éstas introduciendo y generando información para ser consumida por otros individuos, éstos comprando y vendiendo objetos que han sido producidos por otros y éstos jugando con o contra estos o aquellos, "las redes telemáticas son, ante todo, medios de interacción humana, y no simplemente medios de información y comunicación" (Echeverría, 1999, p. 53).

Enumera veinte propiedades esenciales del tercer entorno que lo separan y diferencian de los dos primeros. Las primeras son distinciones matemáticas, otras físicas y otras epistémicas. La primera de todas es que este entorno supone un nuevo marco espacio-temporal socializador. La distalidad y

reticularidad del tercer entorno hace que ya no se hable de reunión, asociación o conversación sino de interconexión. La presencia de los otros deja paso en el tercer entorno a la representación.

> La novedad del tercer entorno estriba en que casi ninguna de las acciones y experiencias que tienen lugar en él requieren la presencia física de los actores, objetos e instrumentos, sino que son llevadas a cabo mediante representaciones tecnológicamente construidas.
> (Echevarría, 1999, p. 65).

La materialidad del los dos primeros entornos se vuelve informacionalidad en el tercer entorno. Éste es informacional, digital, electrónico y virtual. El funcionamiento del tercer entorno *"*no depende tanto de los movimientos de los cuerpos materiales cuanto de la transmisión de una entidad más abstracta, la información, que pasa a "llenar" el tercer entorno" (Echevarría, 1999, p. 74).

La naturalidad, como ya se ha dicho, deja paso a la artificialidad así como lo sincrónico a lo multicrónico. La simultaneidad ya no es necesaria en este espacio social, donde se introduce el *teletiempo.* La extensión, característica de los dos primeros entornos es indiferente en el tercer entorno donde prima la comprensión. Lo importante ahora son las conexiones y los circuitos entrelazados. De este modo, la movilidad física deja así mismo de ser importante en el tercer entorno frente a los flujos electrónicos, y la circulación lenta de los cuerpos deja paso a la circulación rápida de los flujos. El asentamiento en el aire es la característica del tercer entorno lo que supone una inestabilidad continua. La localidad también es desplazada por la globalidad.

Las anteriores eran diferencias físicas (las dos primeras matemáticas) pero existen otras diferencias esenciales entre los dos primeros entornos y el tercero, a saber, de carácter epistémico: pentasensorial versus bisensorial; memoria natural interna versus memoria artificial externa; analógico versus digital; diversificación versus integración semiótica. Dentro de las diferencias sociales destacan: homogeneidad versus heterogeneidad; nacionalidad versus transnacionalidad; autosuficiencia versus interdependencia; y producción versus consumo.

Como nuevo espacio social, el tercer entorno debe ser entendido también como ciudad, como una *pólis* donde los individuos desarrollan sus relaciones humanas, integran y realizan su participación en una comunidad concreta. Esta ciudad es denominada por Echeverría como Telépolis. Ésta se

caracteriza por ser electrónica, digital y tecnológica. Es también una ciudad global o globalizada, en tanto tiende a expandirse a todo el planeta. Al ser artificial, es también inestable, en la medida en que sus cimientos son móviles y cambiantes. En Telépolis surge también una nueva arquitectura donde:

> Internet es la primera gran calle pública de Telépolis [...] Por tratarse de una vía de comunicación a distancia que da cabida a las más variadas formas de interrelación humana, Internet ha de ser considerada como el germen de la sociedad civil de Telépolis.
> (Echeverría, 1999, p. 164).

Por último, Telépolis cuenta también con su propia organización política. La forma de gobierno en esta ciudad es un neofeudalismo, donde los gobernantes deben ser considerados como "señores del aire". Telépolis no es una democracia directa, participativa y global. Los telepolitas no tienen poder de decisión sobre las leyes que rigen la ciudad en la que habitan. Estos señores del aire forman la nueva aristocracia en el tercer entorno, un entorno donde*:*

> Se produce una dura pugna por el poder y la riqueza, que están fuertemente concentradas en las telecuentas bancarias de unos pocos. Ellos son quienes impulsan la construcción y el mantenimiento del tercer entorno y quienes toman las decisiones más relevantes en dicho espacio social.
> (Echevarría, 1999, p. 174)

Por su parte, los telepolitas siguen habitando las urbes del segundo entorno pero emigran hacia el tercer entorno a realizar, cada vez más, las acciones de la vida cotidiana. Son teletrabajadores, telestudiantes, teleociosos, telepacientes, telecuerpos etc. Lo que caracteriza a los telepolitas y los diferencia de los habitantes de los otros dos entornos es que son, principalmente, consumidores. El consumo es esencial para habitar en el tercer entorno, tanto que puede tenerse como el pasaporte hacia este nuevo espacio social. En las siguientes páginas, cuando se trate la gratuidad de Internet, se mostrará la necesidad de consumo para habitar en el tercer entorno.

Con estos dos autores se han querido mostrar los intentos desde la sociología de contextualizar los cambios que las tecnologías digitales han suscitado en las formas de vida humanas. Son dos

propuestas diferentes que convergen en un nuevo modelo de sociedad, de relacionarse con el mundo y con el resto de individuos. Formas de habitar el mundo novedosas y originales de la época digital que llevan a los seres humanos a pensarse a sí mismos y a los otros también de un modo nuevo. La sociedad red del tercer entorno debe aprender a habitar ese nuevo espacio social, así como todas las formas sociales deben adaptarse a él, incluida la filosofía.

1.4.3. Psicología de la sociedad red en el tercer entorno

En 1995 la psicóloga Sherry Turkle escribía *La vida en la pantalla. La construcción de la identidad en la era de Internet.* En esta obra, de carácter etnográfico, construida a través de conversaciones realizadas a jugadores de MUD[16], la psicóloga realiza un estudio sobre el impacto de las TIC e Internet, ejemplificado en este tipo de juegos, en la construcción de la identidad de los individuos. Partiendo de las ideas del posestructuralismo francés, de un yo descentrado y construido a través del lenguaje, realiza un estudio sobre el yo donde aquellas ideas toman cuerpo a través de los medios digitales.

> El yo es múltiple, fluido y construido en interacción con conexiones en una máquina; está hecho y transformado por el lenguaje; el congreso sexual es un intercambio de significantes; y la comprensión proviene de la navegación y el bricolaje más que del análisis. En el mundo tecnológicamente generado de los MUD, me encuentro con personajes que me sitúan en una relación con mi propia identidad.
> (Turkle, 1997, p. 23)

El argumento principal de la obra radica en la idea de una identidad simulada, desdoblada y múltiple. Ante la posibilidad de creación de identidades virtuales o avatares, los individuos construyen personalidades y vidas diferentes a las del primer y segundo entorno. En este entorno artificial y construido, como es el tercer entorno, las identidades de los individuos también son construidas. Acostumbrándose a observar el mundo a través de la pantalla, el individuo construye así mismo su personalidad. Una personalidad múltiple, dividida en tantos caracteres como ventanas tenga delante de la pantalla, "es un lugar [la pantalla] en el que los signos tomados de la realidad sustituyen a lo real" (Turkle, 1995, p. 61). Desde Freud y su idea de un yo descentrado y múltiple hasta la idea lacaniana de un yo como ilusión, Internet ha contribuido a la idea de una identidad

[16] Multi-User Dungeons. El nombre hace referencia a los juegos de rol desarrollado a finales de los años setenta y principios de los ochenta donde los jugadores creaban personajes que podían interactuar entre sí mediante mensajes de texto.

múltiple y cambiante, donde "las personas son capaces de construir un yo merodeador por muchos yos" (Turkle, 1995, p. 227).

La tecnología permite la expresión de una personalidad desdoblada dentro de la normalidad. El sentirse y actuar como otra persona dentro del ciberespacio amplia las barreras de lo que puede ser un individuo sin que le tomen por loco. A los locos ya no se les expulsa de la comunidad como advertía Foucault (1964), pues la realidad virtual y la vida en la pantalla han propiciado la locura dentro de la normalidad. "La creación de personajes en la pantalla, es, por consiguiente, una oportunidad para la autoexpresión, que conduce a que ella se sienta más como su verdadero yo cuando se engalana con una selección de máscaras virtuales" (Turkle, 1995, p. 235). La ilusión y optimismo con los que Turkle trata el tema de la identidad y personalidad son el reflejo de una época marcada por el entusiasmo con el que se acogían a las, por aquel entonces, novedosas tecnologías digitales. Años más tardes y a la vista del camino que éstas han tomado, las preocupaciones respecto a su uso son ahora un tema central para la doctora.

En 2012 Turkle publica *Alone Together*. *Why we expect more from Technology and less from each other?*. En esta obra ya no se trata de ver cómo el ser humano entiende los ordenadores y la tecnología y cómo éstos ayudan a la creación de una identidad. La idea principal es que, actualmente, no sólo cambian aquello que los individuos hacen sino también aquello que son.

En su primera obra, y en aquella época, se entendía la tecnología en términos de estar conectado o desconectado. Una persona entraba en mundos virtuales, estaba más o menos tiempo en el ciberespacio para luego salir de él. Había una frontera clara entre ambos "estados". En la actualidad esa diferencia se ha suprimido casi por completo. A través de los dispositivos móviles, sobre todo por medio de los teléfonos y en concreto de los smartphones, los individuos permanecen siempre conectados.

El problema y tesis principal de la obra de Turkle es que en este mundo de conectividad donde las relaciones humanas también se desarrollan en gran medida en línea, éstas dejan de verse como interacción humana para volverse una acción más del ciberespacio. Ahora es posible, por ejemplo, mantener y conservar una relación familiar o de amistad en la distancia a través de las videollamadas, dando la sensación de que las personas están más cerca y conectadas las unas de las otras. Llamadas que se convierten en presencia (telepresencia para Echeverría) de los interlocutores.

La autora pone el ejemplo de Ellen y su abuela, separadas por la distancia geográfica pero con una relación mantenida por Skype:

> During their Skype conversations, Ellen and her grandmother were more connected than they had ever been before, but at the same time, each was alone. Ellen felt guilty and confused: she knew that her grandmother was happy, even if their intimacy was now, for Ellen, another task among multitasks.
> (Turkle, 2012, p. 24)

Es indudable que la posibilidad de que Ellen y su abuela mantengan conversaciones periódicas mediante la tecnología de las videollamadas constituye una situación que puede entenderse como positiva para ambas partes y que, en este sentido, la tecnología está permitiendo que su relación se mantenga estable y cercana. Pero también es cierto que las relaciones humanas mediadas por la tecnología están siendo vanalizadas en la medida en que se llevan a cabo como una tarea más sin la atención necesaria para una buena socialización y un desarrollo de la empatía.

Constata la autora que las personas comienzan a evitar las relaciones en tiempo real. Las conversaciones, las llamadas de teléfono, las reuniones, etc., son suplantadas por los mensajes de texto, los emails y las videoconferencias. Cada vez más la gente se siente incómoda hablando en tiempo real y en el mismo espacio físico, prefieren la tecnología que les permite "editarse". Cuando se mantiene una conversación presencial entre dos o varias personas, afirma, el individuo habla "sin pensar" en lo que va a decir, el diálogo fluye de tal modo que las personas quedan expuestas ante los demás con las palabras. En un mensaje de texto, en cambio, las personas escriben lo que quieren decir, lo leen, analizan qué pensarán los lectores del mensaje o cómo interpretarán sus palabras y deciden borrar, retocar o mantener lo escrito. De este modo las personas editan sus propios pensamientos, crean la imagen que de ellos mismos quieren transmitir y se crean una imagen para sí mismos de aquello que les gustaría ser:

> At the screen, you have a chance to write yourself into the person you want to be and to imagine others as you wish to them to be, constructing them for your purposes. It is seductive but dangerous habit of mind. When you cultivate this sensibility, a telephone call can seem fearsome because it reveals too much.
> (Turkle, 2012, p 171)

Algo parecido sucede con las redes sociales, que como sucedía con los MUD, permiten a los individuos crearse una imagen de sí mismos y mostrar a los demás esa imagen construida. Desde la elección de imagen personal hasta la información personal que se quiere mostrar, e incluso los sentimientos o pensamientos que se quieren transmitir. Plataformas como Facebook son conscientes de esta situación y dirigen al usuario en esa dirección cuando le sugieren que comunique en qué está pensando, cómo se siente o le permite la introducción de emoticonos[17] a modo de reacción emocional. Las redes sociales permiten a los individuos transmitir una determinada personalidad, unas ideas concretas y una forma de pensar que guste a los que la lean.

Las redes sociales funcionan como "oyentes automáticos". Al colgar algo en una red social se tiene la sensación de que siempre alguien estará escuchando, se espera que alguien lea lo que se ha escrito y que lo marque como "me gusta" dando así una aprobación a la persona que se quiere ser y mostrar. Las redes sociales dan la sensación de llenar un vacío cuando se está solo. Crean una ilusión de compañía y amistad, sin el miedo a la intimidad que ésta requiere.

Para la autora, las conexiones digitales crean tres ilusiones básicas entre sus usuarios. La primera es que permiten al individuo seleccionar la información y de este modo prestar atención sólo a aquello que le interesa de sí mismo y de los demás. En segundo lugar crean la ilusión de ser siempre escuchado. Ésta lleva a la tercera de no estar nunca solo. Las redes sociales y la tecnología online permiten tener la sensación de estar siempre juntos:

> Technology is seductive when what it offers meets our human vulnerabilities. And as it turns out, we are very vulnerable indeed. We are lonely but fearful of intimacy. Digital connections and the sociable robot may offer the illusion of companionship without the demands of friendship. Our networked life allows us to hide from each other, even as we are tethered to each other.
> (Turkle, 2012, p. 13)

Así mismo pone de manifiesto la extendida sensación de entender la soledad como un problema, es una situación que hay que resolver y atajar. Ya no se espera al autobús o a la llegada del metro, no se espera que el semáforo se ponga en verde para cruzar ni la llegada de un amigo a la cita prevista. Las personas se han acostumbrado en estas situaciones a conectarse, a echar mano de sus

[17] Secuencia de caracteres que representan una cara humana expresando una emoción.

dispositivos para no sentirse solos, para no sentirse extraños, o como afirma la autora, para no tener que estar consigo mismos.

Sin embargo, no es cuestión de acabar con las tecnologías digitales ya que un mundo menos conectado resulta ya anacrónico. La idea de la autora es que, en estos "inicios", aun hay tiempo de cambiar el rumbo que están tomando. Un camino que aleja a las personas entre sí y de ellas mismas. Hay que crear espacios para el tiempo real, relaciones en tiempo real y a corta distancia y sobre todo tiempo para la reflexión personal, momentos donde cada uno pueda estar consigo mismo sin sentir miedo de esa compañía.

1.5. La inclusión de los estados en el debate sobre Internet

En mayor o menor medida todos los usuarios-productores de Internet se preocupan por las cuestiones de la ciberética. Google, el objeto de estudio de esta investigación, no es una excepción. Cada vez más, las personas se sienten preocupadas por el uso que se hace de su información, las medidas que toman las empresas implicadas para salvaguardar su intimidad, el grado de censura que existe en el ciberespacio o el problema de las descargas con copyright que se realizan. No es una cuestión en exclusiva de los ciberciudadanos. Empresas y ciudadanos pero también instituciones y organismos gubernamentales entienden la necesidad de prestar atención y entender el ciberespacio como un espacio de convivencia y por tanto de darle una gobernabilidad que suponga un espacio de respeto de los derechos y libertades de las personas.

Con este fin se presentaban en diciembre de 2005 los documentos finales de la Cumbre Mundial sobre la Sociedad de la Información, celebrada entre 2003 y 2005 en Ginebra y Túnez. Entre otras cosas, como el derecho al acceso a Internet, el respeto por los derechos humanos, la asunción de Internet como un medio que permita el empoderamiento de las personas o la necesidad de una red sin interferencias ni injerencias que impidan o disminuyan las posibilidades de las personas, este informe incluye la necesidad de participación de todos los actores implicados en el desarrollo de la Sociedad de la Información. Es decir,

> Los gobiernos, al igual que el sector privado, la sociedad civil, las Naciones Unidas y otras organizaciones internacionales, tienen una función y una responsabilidad importantes en el desarrollo de la Sociedad de la Información y, en su caso, en el proceso de toma de decisiones. La construcción de una Sociedad de la Información centrada en la

> persona es un esfuerzo conjunto que necesita la cooperación y la asociación de todas las partes[18].

El 16 de mayo de 2011 la Asamblea General de Naciones Unidas publicaba su decimoséptima sesión sobre la promoción y protección de los derechos humanos, en concreto sobre la libertad de expresión. El objetivo de la misma era explorar

> key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet. The Special Rapporteur underscores the unique and transformative nature of the Internet not only to enable individuals to exercise their right to freedom of opinion and expression, but also a range of other human rights, and to promote the progress of society as a whole[19].

Un año más tarde, en su veinteava sesión, se reiteraba la importancia de la promoción y defensa de los derechos humanos y en concreto de la libertad de expresión en Internet. El Consejo de Derechos Humanos:

1. Afirma que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos;
2. Reconoce la naturaleza mundial y abierta de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas;
3. Exhorta a los Estados a que promuevan y faciliten el acceso a Internet y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países;
4. Alienta a los procedimientos especiales a que tengan estas cuestiones en cuenta en sus mandatos actuales, según proceda;

---

[18] https://www.itu.int/net/wsis/outcome/booklet-es.pdf

[19] http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

5. Decide seguir examinando la promoción, la protección y el disfrute de los derechos humanos, incluido el derecho a la libertad de expresión, en Internet y en otras tecnologías, así como la forma en que Internet puede ser un importante instrumento para el desarrollo y para el ejercicio de los derechos humanos, de conformidad con su programa de trabajo[20].

En 2014 el Comité de Naciones Unidas por los Derechos Humanos incluía entre sus tres puntos fundamentales de la reunión (sesión número 110) su preocupación por la privacidad e intimidad de las personas en Internet.

> I address you today to continue to seek your support on three issues which are of current importance not only to this Committee but also for the promotion and protection of human rights more generally. The first is the right to privacy in the digital age. Powerful new technologies offer the promise of improved enjoyment of human rights, but they are vulnerable to mass electronic surveillance and interception. This threatens the right to privacy and to freedom of expression and association [...] In December of last year, Member States of the General Assembly adopted a resolution expressing their deep concern at the negative impact that surveillance and interception of communications may have on human rights. This resolution calls on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data[21].

Estas son algunas muestras de cómo los gobiernos y sus organismos están tomando en consideración la necesidad de dirigir las miradas hacia el ciberespacio e Internet. Desde los primeros intentos de la comunidad científica y académica hasta la inclusión de estas instituciones en los debates entorno a la necesidad de una legislación y una ética en internet ha pasado casi medio siglo. Un tiempo durante el cual el desarrollo de la tecnología y el ciberespacio ha ido siempre por delante de los gobiernos, las instituciones y las comunidades involucradas.

Tal vez el motivo de esta descoordinación se deba a que la industria tecnológica avanza a una velocidad mayor o, mejor dicho, a un ritmo más constante que el pensamiento sobre ella. Si como

---

[20] http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf

[21] http://webcache.googleusercontent.com/search?q=cache:jXF1jiLDZooJ:tbinternet.ohchr.org/Treaties/CCPR/Shared%2520Documents/1_Global/INT_CCPR_OCR_110_21769_E.doc+&cd=3&hl=es&ct=clnk&gl=es

afirma Virilio (1997) la cuestión de la velocidad es una cuestión de democratización, es necesaria una adecuación entre ambos ritmos que permita la inclusión de la democracia en el ciberespacio. De ahí la necesidad de la comunidad científica de crear un marco de actuación al cual las empresas y la tecnología tengan que ajustar sus invenciones. No se trata de poner freno a la invención tecnológica y al avance de nuevos servicios y herramientas digitales sino de conseguir que se haga de un modo respetuoso con todos los agentes involucrados.

Del mismo modo que los derechos humanos, la legislación y los acuerdos internacionales sobre la gobernabilidad de los pueblos no está encaminado a la ralentización o la disminución de la instauración de comunidades, los derechos digitales y la gobernabilidad del ciberespacio tampoco persiguen ese fin. El objetivo de la ciberética y la legislación de este espacio tienen como objetivo precisamente la creación de las condiciones de posibilidad de un espacio digital sólido y fuerte, que pueda mantenerse y sobrevivir a su propia evolución de un modo democrático para todos sus miembros.

En las siguientes páginas se analizará un concepto central para la ciberética, que es la cuestión de la privacidad. Como se ha ido viendo, existen muchas otras preocupaciones relacionadas con el ciberespacio e Internet. La propiedad intelectual, el derecho de software, responsabilidad profesional, acceso y autonomía, la vigilancia y censura, etc. Pero, de un modo u otro todas estas preocupaciones convergen en la privacidad, de ahí que sea el tema central de esta investigación.

Las definiciones aportadas serán aquellas que ha dado la propia ciberética y la ética informática y no tanto las históricamente admitidas. La privacidad no es un concepto nuevo de las tecnologías digitales, como podrían ser los derechos de software, y su trayectoria histórica es más amplia que la que aquí se expondrá. En las siguientes páginas se tratará la privacidad desde la perspectiva de la ciberética, por lo tanto no es de esperar que se traten teorías anteriores al nacimiento de la misma. Si bien es cierto que las diferentes posturas vienen determinadas por tradiciones éticas concretas, se considera que no es necesario extenderse en todas y dejar a las propias teorías nuevas explicar y argumentarse por sí mismas.

En cualquier caso, cuando sea necesario para la argumentación o exposición de las visiones aquí tratadas podría haber alguna referencia a tradiciones anteriores a modo de apoyo o aclaración conceptual, pero siempre de una manera secundaria. Una vez analizada cada postura se realizará el

mismo ejercicio con Google, con la intención de mostrar en qué medida se acerca o aleja a las diversas teorías. Así mismo se pretende mostrar el modo en que atiende a las necesidades del ciberespacio, si contribuye a la consolidación de una ética y cuáles pueden ser las diferencias entre lo que la ciberética propone y las actuaciones de Google.

CAPÍTULO 2:
INTERNET INMATERIAL,
LIBRE Y GRATUITO

Se tiende a pensar en Internet como un espacio sin lugar físico, gratuito, libre y democrático. La proliferación de las conexiones wifi hacen que cada vez sea más fácil conectarse a Internet. La nube, esa nueva forma de gestionar la información desde cualquier lugar y con acceso desde cualquier dispositivo apoya esa noción de no lugar o, más bien, la noción de "en cualquier parte". Cualquiera, en cualquier lugar y momento puede conectarse a la red. A continuación se analizan estos supuestos a fin de poder comenzar la investigación central de este trabajo sobre la privacidad en el ciberespacio y las prácticas llevadas a cabo por Google a este respecto. Si bien es cierto que Internet puede dar la impresión de ser una red inmaterial, que no es necesario ningún tipo de gasto para su uso y que en ella impera la libertad, también es cierto que estos supuestos son sólo aparentes y que detrás de ellos emerge una red que no es la que parece.

2.1. Internet como un espacio inmaterial

La red, Internet o el ciberespacio, se presenta al usuario como algo sin espacio definido. La idea de que la conectividad a Internet está en todas partes alimenta esta opinión sobre su inmaterialidad. Desde casa o el trabajo, desde los espacios públicos y los establecimientos, en cualquier momento uno puede conectarse sin dificultad a Internet. En este sentido se puede afirmar que efectivamente Internet es un no-lugar, o tal vez debería expresarse como un "en todas partes".

De cualquier modo, se exprese como se exprese, lo cierto es que Internet sí ocupa un lugar físico en el mundo. Esta materialidad comienza, desde lo más básico, con los dispositivos mediante los cuales se navega por la red, a los que se tienen que añadir los elementos que permiten que las señales se transmitan, esto es, las antenas, satélites y cables submarinos que proporcionan la señal necesaria para hacer efectiva una conexión.

Mientras antes era posible afirmar la existencia de dispositivos electrónicos que no estuvieran conectados a Internet, a medida que avanza la tecnología cada vez es más frecuente la inclusión de esta red en cualquier tipo de dispositivo electrónico. Relojes, lavadores, hornos, coches, sistemas de seguridad en los hogares, asistencia sanitaria y un largo etcétera son algunas de las nuevas introducciones en esta red de interconexiones que permiten ser controlados de modo remoto.

Estos aparatos, que cada vez más rápido se quedan anticuados y obsoletos por la aparición de otros más sofisticados, entendiendo aquí sofisticados como más conectables, son reemplazados por estas nuevas versiones. Estos viejos dispositivos contienen multitud de componentes y ocupan un espacio

real en el planeta. Un espacio que cada vez está más lleno. Esto ha dado lugar a que los RAEE (Residuos de aparatos eléctricos y electrónicos) o e-waste se estén convirtiendo en un problema medioambiental. Según datos de Greenpeace[22] se generan al año unas 50 millones de toneladas al año de RAEE. Hace ya seis años, en 2010 se estaban estrenando 716 millones de ordenadores en todo el planeta, sólo China tenía 178 millones de nuevos usuarios de ordenadores e India 80 millones. Todos estos nuevos dispositivos, junto con los ya existentes y otros aparatos electrónicos usados para navegar por la red ocupan un lugar en la tierra, un lugar real, tangible y visible.

Este espacio ocupado por la basura electrónica representa sólo el de los dispositivos que se utilizan para navegar por Internet. Se podría afirmar que la existencia de todos estos aparatos no significa todavía que la red o Internet ocupen un lugar físico concreto. Pero cuando se afirma que el ciberespacio ocupa un lugar físico, no se hace referencia (sólo) a estos aparatos. A éstos hay que añadirle la red en sí, que lejos de ser algo etéreo y a-espacial, ocupa un espacio muy real.

La información que se puede obtener en Internet no está en la red, esperando a que se requiera para aparecer ante una pantalla. Toda la información contenida en ella está alojada en un lugar físico. Puede estar alojada en pequeñas cantidades en espacios reducidos, como ordenadores o redes de datos (físicas) o en enormes cantidades como en los "data centers" o centros de procesamiento de datos (CPD). Sólo en España existen 58 centros de este tipo[23]. En este último caso ocupan un espacio físico evidente. En algunos casos, son conjuntos de edificios, agrupaciones del tamaño de pequeñas ciudades, donde se almacenan grandes cantidades de información. De hecho, la nube, esa metáfora utilizada para mantener lo etéreo de Internet, no es otra cosa que CPDs que almacenan grandes cantidades de datos que después se pueden recuperar a través de Internet.

Se podría seguir argumentando que aunque la información ocupe un espacio concreto y aunque se necesiten aparatos para conectarse a Internet eso no significa que, efectivamente, la red ocupe un espacio concreto y que la información almacenada en los CPDs y que llega a los apartados lo hace de un modo tal que no ocupa un lugar físico. Si bien es cierto que la información viaja sin ocupar, aparentemente un espacio concreto, también es cierto que son necesarias canalizaciones, vías por las que esa información pueda viajar.

---

[22] http://www.greenpeace.org/espana/es/Trabajamos-en/Parar-la-contaminacion/Electronicos/El-problema/. Consultado el 15 de agosto de 2016

[23] http://www.centrodedatos-datacenter.es/

Del mismo modo que se necesitan antenas y repetidores para ver la imagen en la pantalla de un televisor o un cable que conecte un teléfono a otro, con la información e Internet sucede lo mismo. Sin tener en cuenta los satélites y las antenas, que ocupan sin lugar a dudas un espacio concreto, están los cables submarinos de fibra óptica. La fibra óptica consiste, a grandes rasgos, en enviar pulsos de luz que representen datos a transmitir. Permite enviar grandes cantidades de datos entre lugares muy alejados entre sí. Alcanza la velocidad de la radio y velocidades muy superiores al cable normal o al satélite, de ahí que sea utilizado ampliamente en las telecomunicaciones.

Un motivo del auge de la fibra óptica en detrimento del satélite (utilizado todavía hoy para las comunicaciones pero que está siendo desplazado por ésta) estriba en que mientras para realizar una conexión (ya sea una llamada, un mensaje instantáneo, una búsqueda en Internet o comprobar el correo personal) vía satélite se tienen que recorrer 36.000 kilómetros para hacerlo, pues la señal debe dirigirse al satélite, que orbita el planeta y éste volver a trasmitirla a la Tierra, con fibra óptica se necesita tan sólo la distancia que haya entre repetidor y repetidor.

Esta disminución de la distancia y el abaratamiento de las comunicaciones son motivos suficientes para crear una red de cables submarinos que conecten, básicamente, todas las partes del mundo y que permitan una comunicación a nivel global de un modo rápido. Por poner un ejemplo, el SeaMeWe-3 tiene una longitud de 39.000 km y atraviesa cuatro continentes, desde Norden en Alemania hasta Keoje en Corea del sur y Perth en Australia (en Singapur el SeaMeWe-3 se bifurca hacia el norte, abarcando Malasia, Filipinas, Vietnam y China y hacia el sur llegando a Australia)[24].

Con esa longitud, creado y usado en exclusiva para las telecomunicaciones vía Internet, con todos los aparatos electrónicos que se utilizan para navegar, con la basura electrónica que aumenta a la misma velocidad que aparecen nuevos dispositivos, etc., decir que el ciberespacio no ocupa un lugar determinado es cuanto menos osado. Claro está que toda la biblioteca de Alejandría cabría en un dispositivo ridículamente pequeño en comparación con el espacio que ocupaba la famosa biblioteca. Siendo capaces de disponer de más información en la palma de la mano de la que nunca hubo en aquel edificio es fácil pensar que la red no ocupa lugar. Pero lo cierto es que sí ocupa lugar, y uno muy amplio.

---

[24] http://www.smw3.com/

2.2. La gratuidad de Internet

Está muy extendida la idea, debido en gran parte a la idea de no-lugar, que Internet es gratuito. El "Registrarse es gratis y lo será siempre" de Facebook es un eslogan que pone de relieve esa idea de gratuidad de Internet. Salvo en la compra en línea, donde se tiene que realizar una transacción económica y el usuario es consciente de esa transacción, navegar por la red no requiere de ningún desembolso de dinero. Esta es la primera impresión que uno tiene de Internet.

Un análisis rápido advierte enseguida que esto no es cierto. El hecho de utilizar Internet sin tener que pagar por ello al momento no significa que sea gratuito. El caso más evidente y palpable es el dispositivo con el que se navega por la red. Ordenadores, tabletas, teléfonos y relojes inteligentes, televisores, etc., son algunos de los dispositivos de los que se ha de disponer si se quiere navegar por la red.

Estos aparatos por sí solos no ofrecen conexión a la red. Es imprescindible la compra o subscripción a una conexión a Internet, una línea que permita el enlace entre el dispositivo e Internet. De este modo es necesaria la contratación de esa líneaa una empresa proveedora de servicios de Internet. Este son los primeros gastos que tendrá que hacer un usuario para conectarse a Internet; dispositivo y conectividad. Visto de este modo, navegar por la red no es gratuito.

Puede pensarse que el hecho de navegar por Internet desde un lugar público como puede ser una biblioteca o un cibercafé con un dispositivo propiedad del establecimiento significa que Internet es gratuito. Pero el hecho de que un cibernauta no pague ni por el dispositivo ni por la conexión no implica que ambas cosas sean gratis, tan sólo que esa persona en cuestión no ha pagado por ninguna de ellas. Del mismo modo que utilizar la conexión del vecino para conectarse a Internet no significa que sea gratis, sino que se está robando la conexión al vecino.

Existen otro tipo de pagos que el usuario hace, ya no *para* sino *al* navegar por Internet. De éstos se hablará más adelante, siendo un tema capital para esta investigación. Ahora tan solo señalar que estos pagos no serán pagos que supongan un gasto económico para el usuario, sino más bien humano. La privacidad, vigilancia, censura, etc., que se pueden ejercen sobre el usuario al navegar por la red pueden ser consideradas formas de pago. Como también pueden serlo la esclavitud y explotación a la que se somete a miles de personas para la producción de los dispositivos y la contaminación y presión ambiental que se ejerce sobre el planeta para mantener el ciberespacio.

Este tipo de pagos, sobre todo los relacionados con la privacidad de las personas en el ciberespacio, son centrales para esta investigación. En ellos se basa la gratuidad de las herramientas y servicios que ofrece Google a sus consumidores-usuarios, así como su fuente de ingresos. Esto se tratará en extensión en el capítulo dedicado a la privacidad en Google, cuando se analice su Política de privacidad frente a las diversas teorías éticas relacionadas con la privacidad en el ciberespacio.

2.3. La libertad y democracia en Internet

Como medio de expresión por el cual los cibernautas pueden opinar, mostrar su conformidad y disconformidad con un tema cualquiera, unirse y ejercer presión sobre un asunto, etc., se consideran el ciberespacio e Internet espacios libres y democráticos. Un ejemplo sobre la controversia que puede acarrear el tema de la libertad y la democracia será suficiente, de momento, para observar cómo la cuestión no tiene una respuesta fácil. La detección de una red de pederastia viene determinada por la capacidad de la policía de interceptar determinados mensajes, fotografías e información almacenada en dispositivos particulares y por lo tanto de la posibilidad del cuerpo del estado de vigilar las comunicaciones privadas, lo que se considera un atentado contra la libertad y la democracia digital. Este ejemplo se puede extender al acoso escolar o la violencia de género, que sin ser inherentes al nuevo espacio cibernético, adquieren en éste unas dimensiones hasta ahora desconocidas y su violencia se amplia en tanto se amplia la capacidad de dispersión. Es la característica de memoria artificial externa del tercer entorno lo que permite perseguir este tipo de maltrato y acoso por un lado, pero también vigilar y censurar a los ciudadanos.

La vigilancia, el seguimiento y la censura en Internet puede suponer, por un lado la libertad y la democracia para algunos miembros de la comunidad cibernética, y la represión y la tiranía para otros. La ciberética y por ende esta investigación trata de buscar y marcar los límites para hacer de Internet un espacio libre y democrático para todos. La cuestión no es fácil en la medida en que la comunidad se compone de muchas y muy diversas formas de pensar y el relativismo cultural que tanto teme la antropología se convierte en el ciberespacio en el ser de la propia comunidad.

Debido a este relativismo cultural, en tanto que la aldea global no se compone de un solo referente cultural y que las personas que la componen están inmersas en su propio marco referencial, se presupone que Internet es un espacio libre. Uno puede navegar por la red sin limitaciones; hablar con alguien lejano incluso sin conocerse nunca; participar de la política y de acciones ciudadanas; participar de un mundo virtual donde uno es lo que quiere ser; comprar droga y armas; decir y hacer

lo que a uno le apetezca sin atenerse, en un primer momento a las consecuencias de los actos. La distancia espacial, esa mediación de la comunicación a través de un dispositivo que aleja al individuo de la alteridad (que ya se veía en Turkle), del otro al que está dirigida cualquier acción comunicativa permite esa sensación de libertad.

Esta libertad se puede interpretar de muchas y diferentes maneras. Libertad puede significar para algunos la capacidad para navegar por la red, disponer de un dispositivo y de una conexión a Internet. Para otros, libertad puede entenderse como la posibilidad de hacerlo sin restricciones. Libertad puede significar también la posibilidad de realizar acciones que de otro modo serían imposibles; se puede hablar con alguien en Quebec mientras se está en Barcelona; se puede visitar el Louvre sin haber estado nunca París; se puede ser un orco por la tarde y levantarse al día siguiente para dirigir un país, etc. Estos ejemplos, que no son lo únicos, son los utilizados para afirmar que Internet es un espacio libre; uno es libre de hacer lo que quiera hacer sin limitaciones de ningún tipo. A pesar de esto, se podría seguir pensando que Internet no hace libres a las personas pero es necesario afirmar que ha ampliado las posibilidades de serlo o cuanto menos de sentirse.

Aunque esta investigación no pretende ser un análisis de la libertad en Internet propiamente dicha, muchos de los temas que se tratarán convergen con ella. Por ello es necesario señalar algunos aspectos relativos a aquélla que permitan situarla dentro del espacio de Internet.

Desde hace unos años Reporteros Sin Fronteras (RSF), ONG encargada de velar por la libertad de prensa y de expresión, incluye en sus misiones la observación de la censura y la vigilancia en Internet. Cada año, coincidiendo con el día de la libertad de expresión, publica un informe donde reporta la situación de ésta en el mundo y desde hace unos años también en la red. Este informe, llamado "Los enemigos de Internet" incluye datos relevantes para contextualizar la libertad en Internet.

En el informe de 2014[25] RSF clasificaba 32 instituciones enemigas de Internet; instituciones que vigilan de una forma activa e intrusiva el ciberespacio. El informe trataba sobre instituciones enemigas de Internet y no sobre países, como se había hecho en anteriores documentos. Los motivos de este cambio es que "señalar como *Enemigos de Internet* a instituciones más que a Estados permite poner en evidencia la esquizofrenia de ciertos países cuando se trata de la libertad

[25] http://www.rsf-es.org/

en línea"[26]. Lo que se pretende señalar es que existen países como Korea del Norte, Emiratos Árabes Unidos, Arabia Saudí, Bahreín, Sudan o Siria donde opera más de una institución de vigilancia y censura, de ahí que expresarse en términos de países no dejaría ver la magnitud de la situación. Cierto es que estos países no se caracterizan por ser democracias y un defensor de la idea de libertad en Internet podría afirmar que el problema de estos países es la poca libertad que hay en estos países, dentro y fuera de la red.

Aunque esto es cierto y es fácil suponer que en un país donde no existe la libertad de expresión o de reunión tradicionales tampoco existirán esas libertades en el ciberespacio, sucede que esas instituciones, y de aquí también radican los motivos por los que RSF quiso, en este informe, desmarcarse de los países para centrarse en instituciones, están también en países considerados como democracias. Más concretamente, India, Estados Unidos y Reino Unido. Estas instituciones gubernamentales, instituciones que dependen de un modo directo de la financiación, la logística y en definitiva del apoyo de las instituciones públicas de estos países son, respectivamente, el Centre for Development of Telematics (C-DOT), la National Security Agency (NSA) y los Government Communications Headquarters.

Aunque se haya dejado de hablar de países para hablar de instituciones lo cierto es que esas instituciones pertenecen y/u operan en países. De hecho, el número de éstos que de un modo u otro gestionan, financian, contratan, participan, aprueban o apoyan estas instituciones enemigas de Internet asciende a 22[27]. Esto significa que no sólo estos tres países permiten a esas instituciones trabajar en sus territorios, sino que hasta 19 países más contratan a estas empresas para llevar a cabo acciones de espionaje y vigilancia contra sus propios ciudadanos. Estos países son considerados como enemigos de Internet en la medida en que son estados que practican una vigilancia activa e intrusiva y permiten de un modo explícito graves violaciones de la libertad de información y de los derechos humanos[28].

Además de países e instituciones enemigas de Internet, RSF habla de "mercenarios de la vigilancia". Estos mercenarios son aquellas empresas especializadas en interceptar comunicaciones

---

[26] http://12mars.rsf.org/2014-es/enemigos-de-internet-2014-las-instituciones-en-el-nucleo-del-sistema-de-censura-y-vigilancia/

[27] idem.

[28] http://surveillance.rsf.org/es/

y bloquear contenidos en Internet. Bloquear contenidos relacionados con la pedofilia, la violencia, el racismo o cualquier actividad que vulnere los derechos de las personas puede ser tenido como un bien o como una acción por el interés público. Pero lo que denuncia RSF es que esta vigilancia, seguimiento y censura se realiza, en muchos casos, de un modo indiscriminado, a todas los ciudadanos y ciudadanas de un lugar concreto y muchas otras veces simplemente a personas con ideas contrarias a los intereses particulares de unas personas o instituciones.

Tres empresas destacan sobre las existentes en el informe publicado, ISS Mundial, Milipol y Technology against Crime. ISS World, se ofrece en su web como "Intelligence Support Systems for Lawful Interception, Electronic Surveillance and Cyber Intelligence Gathering"[29]. Milipol, por su parte, se anuncia como un congreso internacional para la "seguridad interna de los Estados"[30] y Technology against Crime lo hace como un congreso internacional en tecnología para un mundo más seguro[31]. Según RSF, estas empresas, entre otros servicios, tienen como uno de sus objetivos centrales el abastecimiento a las instituciones públicas y privadas de los países las herramientas necesarias para la vigilancia de sus ciudadanos. Así que, teniendo en cuenta las afirmaciones de RSF, afirmar que Internet es un lugar libre puede y debe, cuanto menos, matizarse.

De hecho, matizar tal vez sea insuficiente para hablar de libertad en el ciberespacio. Según RSF en marzo de 2014 habían muerto 21 cibernautas y 174 más estaban encarcelados por participar y/o contribuir de algún modo a defender la libertad de expresión en Internet, bloggers, net-disidentes, activistas, reporteros de medios digitales, etc.[32] Sus crímenes son precisamente, en gran medida, ejercer de un modo u otro la democracia en Internet.

Es precisamente la vigilancia y seguimiento del usuario medio lo que lleva a la ciberética a preguntarse por las condiciones de posibilidad de vulnerar derechos de los ciudadanos a través y en el ciberespacio. No se trata de que agencias de inteligencia se espíen unas a otras o que se persiga el crimen o el terrorismo en la red. La cuestión básica que se plantea la ciberética, en este sentido, es la necesidad de marcar unas pautas de actuación en el ciberespacio que permitan la seguridad de las personas y los estados al tiempo que respeten las libertades individuales de los ciudadanos en un

---

[29] http://www.issworldtraining.com/

[30] http://www.milipol.com/

[31] http://www.forum-tac.com/en/

[32] http://www.rsf-es.org/informes/

mundo conectado cibernéticamente. Que la tecnología permita la vigilancia masiva de los internautas no significa que éstos deban ser vigilados por defecto. Deben existir unos mecanismos de control que permitan a los cibernautas vivir en el ciberespacio, al menos, en el mismo grado de seguridad y libertad que viven en el espacio no cibernético.

El año 2001 marcó, sin lugar a dudas, un hito en cuanto a la seguridad nacional de los países y movió las fronteras sobre lo que se considera intimidad personal y su vulnerabilidad o respeto. En nombre de esa seguridad nacional, países, instituciones y organismos se han servido del acceso a la información y de la falta de regulación al respecto para vigilar y seguir las comunicaciones de los ciudadanos. Qué lugares web se visitan, desde qué tipo de ordenador, desde qué lugar, qué se envía, cuelga, comparte, tuitea, contesta y, en general, cualquier movimiento que se haga en la red. Internet está tan inserto en la vida y acciones diarias de los ciudadanos que no se trata ya en exclusiva de sus movimientos en la red sino de cualquier aspecto de la vida diaria de las personas, qué tipo de trabajo se realiza, qué alimentos se consumen, dónde y cuánto cuesta consumirlos, dónde se viaja, por qué medios de transporte, qué religión se procesa, qué hábitos culturales se tienen, etc. El alcance de la información personal contenida en la red es tan amplia como la vida de las propias personas que la componen.

La censura opera en todos estos niveles. El caso de WikiLeaks supone un claro ejemplo de vigilancia y censura, al mismo tiempo que introduce la cuestión sobre la idea de democracia de Internet, a menudo confundida con la idea de libertad que se mostraba más arriba y que ha quedado evidenciada como una libertad carente de muchos aspectos que, en principio, debiera contener.

El caso de WikiLeaks, Julian Assange o Chelsea Manning son solo la cara más visible, mediática y de mayor envergadura de unas acciones que se repiten a lo largo del ciberespacio y que muestran la necesidad de la ciberética en el debate sobre Internet, la necesidad de pensar cómo gobernar el ciberespacio para hacer de él un lugar seguro y habitable para todos sus ciudadanos. Estos casos pusieron al descubierto y mostraron a los usuarios de las telecomunicaciones que estaban siendo vigilados de forma masiva e indiscriminada, sin motivos suficientes ni justificados. Por otra parte mostraron la vulnerabilidad de la privacidad en el ciberespacio y pusieron de manifiesto cierta alegalidad del ciberespacio y la falta de una cultura democrática en la red.

No se pretende aquí explicar el caso de WikiLeaks que dio la vuelta al mundo y que fue portada en los medios de comunicación durante el tiempo suficiente para que toda persona sea conocedora del caso. Tan solo mostrar cómo funciona la censura en Internet siendo éste un caso de divulgación de espionaje masivo. Pudiera parecer que el caso, por su envergadura, es un caso excepcional y que la censura no opera del mismo modo en un caso particular, como puede ser un disidente político o un ciberactivista. Pero, hay que hacer un ejercicio intelectual y no quedarse con el ejemplo particular sino ver el caso en su conjunto; centrarse en los mecanismos disponibles en la red para la censura y lo rápido y fácil que puede acabarse con la libertad de prensa y expresión en el ciberespacio.

El 28 de noviembre de 2010 WikiLeaks sacaba a la luz Cablegate. Un cuarto de millón de comunicaciones entre el Departamento de Estado de los Estados Unidos y sus embajadas en el exterior. Ya antes de esta filtración se habían realizado otras por parte de WikiLeaks, como fueron los documentos filtrados sobre las guerras de Afganistán o Irak. En este caso, con el Cablegate, no se trataba de la actuación de un país o países en una guerra sino de documentos que probaban la injerencia en la soberanía de los países y de éstos sobre sus ciudadanos a través de la vigilancia.

De España, por ejemplo, aparecían cuestiones relaciones con el caso de la muerte del periodista José Couso durante la guerra de Irak; la autoría del 11-M y el interés y seguimiento de la vulneración de los derechos de propiedad intelectual a través de las webs de descarga de contenido. De Egipto, estos documentos afirmaban que la revolución, que finalmente vio la luz en 2011 y que sería conocida como parte de la primavera árabe, habría comenzado años antes a través de los cibernautas quienes habrían ido preparando el terreno para la derrota de Mubarak en 2011. Estos cables afirman la existencia, desde 2006, de una conexión entre los cibernautas egipcios y tunecinos y mostraban cómo las redes sociales habrían ayudado de un modo considerable la revolución árabe .

Siendo una causa global, que afectaba a la mayoría de los países "conectados" la respuesta fue contundente y rápida. Inmediatamente después de la filtración de los cables, WikiLeaks es víctima de DDoS (ataques de denegación de servicio[33]) por lo que decide albergarse en la nube de Amazon. El 1 de diciembre el gobierno de la República Popular China bloquea los enlaces a WikiLeaks y Amazon cancela su acuerdo. Un día más tarde EveryDNS (proveedor de servicios) deja de

[33] Es un ataque a un sistema de computadoras o red que causa que un servicio sea inaccesible a los usuarios.

proveerle acceso a Internet y OVH es presionada para que haga lo mismo en Francia, cosa que acaba haciendo. Es entonces cuando el partido Pirata suizo ofrece a WikiLeaks alojamiento web[34].

El 4 de diciembre PayPal cancela la cuenta vinculada a la organización por la cual WikiLeaks recibía fondos para su financiación. El 6 de diciembre se unen al bloqueo MasterCard y PostFinance. Ese mismo día Anonymous, en defensa de WikiLeaks, activa la Operation Payback realizando ciberataques a Paypal y PostFinance por haber cancelado las cuentas de ésta. Visa cancela la posibilidad de pagos a WikiLeaks el 7 de diciembre. Dos días más tarde Twitter decide cancelar la cuenta de Anonymous por el apoyo que ofrece en esta red social al trabajo de WikiLeaks. Facebook hace lo propio con el perfil de Operation Payback.

Todo ello sucede en un período de diez días. En poco más de una semana WikiLeaks deja de recibir soporte en la red, con motivo de haber divulgado la vigilancia masiva en el ciberespacio. Ésta, la posterior censura y manipulación y la criminalización de la denuncia de estas conductas no encajan en las características de un entorno democrático. Lo que sucede es que Internet no es un espacio democrático. Cuando Echeverría (1999) define el tercer entorno, la forma de gobierno que le asigna a este nuevo espacio social es la de un neofeudalismo, donde los países y gobiernos han perdido su poder y soberanía frente a estos nuevos señores feudales.

> Contrariamente a quienes piensan que Internet realiza el ideal de una democracia directa y global, en esta obra se afirma que, en su situación actual, las decisiones principales concernientes a la construcción de dicha urbe telemática escapan por completo al control de los telepolitas [...] Las decisiones fundamentales sobre la cosntrucción del tercer entorno no las toman los Estados en su autonomía y soberanía [...] Los estados no tienen el monopolio de la violencia en E3 (tercer entorno), puesto que muchas empresas multinacionales pueden llevar a cabo operaciones agresivas en el entorno telemático sin control de los Estados.
> (Echeverría, 1999, pp. 174 y 183)

Sin embargo, a pesar de que después de lo dicho resulta difícil de hablar de libertad en Internet, existen espacios creados por los ciberciudadanos que permiten albergar cierta esperanza para la

[34] Es el servicio que provee a los usuarios de Internet un sistema para almacenar información de cualquier tipo accesible mediante web.

libertad y la democracia en la red. El ciberactivismo ha supuesto la creación de comunidades virtuales que crean grupos de presión reales, encaminados a reforzar los derechos y libertados de los ciudadanos, dentro y fuera del ciberespacio.

2.3.1. Ciberactivismo

Estas preocupaciones sobre el entorno digital tienen su respuesta en lo que se puede definir como ciberactivismo. La idea del ciberactivismo parte de utilizar las tecnologías digitales, y sobre todo Internet, con el fin de organizarse y crear un lobby frente a situaciones negativas para determinados grupos que por otros medios no tendrían la fuerza suficiente para ser escuchados o tendrían menor repercusión a escala global. Asociaciones como Oxfam Intermon, Amnistia Internacional o Greenpeace se han apoyado en plataformas digitales parar realizar algunas de sus campañas.

Además de ONGs existen otros grupos y organizaciones que realizan ciberactivismo. Entre ellos se encuentra la Electronic Frontier Foundation. Creada en 1990 por Mitch Kapor, John Gilmore y John Perry Barlow, que se conocieron en la comunidad virtual The WELL, organización pionera en el ciberactivismo[35]. Su misión es "champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows"[36].

Sus logros son muchos e importantes en este sentido, como la protección del software como derecho de libertad de expresión y ausente de posibles censuras; revocar la doctrina Betamax por la cual se frenaba la innovación tecnológica al considerar que los distribuidores de *peer to peer*[37] vulneraban los derechos de propiedad de Hollywood; o la protección ante las lecturas, por parte de gobiernos y organismos, de correos electrónicos sin una orden judicial.

Existen más ejemplos, como plataforma europea denominada Europe Vs. Facebook. Su trabajo se centra en la protección de los usuarios europeos de esta red social pero, como ellos mismos afirman "We happened to look at Facebook for a number of reasons but the results are very likely exemplary

---

[36] https://www.eff.org/about

[37] Peer to peer es una red de ordenadores en la que cada uno de ellos actúa como servidor y cliente respecto a otros ordenadores. Estas redes permiten el intercambio de información directo entre todos los ordenadores conectados.

for a whole industry"[38]. Entre sus objetivos se encuentran: el respeto a la protección de datos por parte de las empresas de Internet; hacer frente ante las políticas de privacidad imprecisas; la accesibilidad fácil e inequívoca a las políticas de privacidad de las plataformas y al uso de los datos personales de los usuarios; la protección ante la forma abusiva de compartir información entre las diversas plataformas de una misma empresa o compañía sin la autorización expresa del usuario; o acabar con el mantenimiento de información personal de los usuarios sin su aprobación, incluso cuando éstos ya se ha dado de baja en los servicios o han expresado su deseo de eliminar determinado contenido.

Otro ejemplo de ciberactivismo, tal vez el más conocido de ellos, es la organización Anonymous. La organización conocida por la máscara de Guy Fawkes realiza acciones de denuncia o protesta contra la vulneración de los derechos humanos y ataques contra organizaciones que puedan poner en peligro el derecho a la libertad de información. Han realizado acciones contra el canon digital, la censura de Wikileaks, el cierre de Megaupload, apoyando las revoluciones en los países árabes, contra las leyes antipiratería, etc. Así mismo se han pronunciado contra grupos terroristas como ISIS tras el atentado a la editorial de Charie Hebdo en enero de 2015 y los atentados de París de noviembre del mismo año.

Estos son tan solo unos ejemplos del ciberactivismo pero no son los únicos. Change.org, CitizanGo o Avaaz.org, por ejemplo, son páginas web dedicadas a la recolección de firmas con el objetivo de protestar o denunciar determinadas acciones gubernamentales. Su funcionamiento se basa en la idea de la unión de personas individuales en un colectivo lo suficientemente amplio como para constituirse como grupo de presión frente a una situación determinada. En diciembre de 2015 Avaaz.org contaba con más de 42 millones de miembros activos y más de 267 millones de acciones[39]. Por su parte, en Chage.org habían firmado peticiones en esa misma fecha más de 130 millones de personas[40]. A la luz de estas cifras se observa que el ciberactivismo es el medio por el cual las personas pueden denunciar o dar apoyo a situaciones que, sin las herramientas informáticas y cibernéticas, sería imposible llevar a cabo, o cuanto menos no tendrían tanto impacto como el que pueden alcanzar por este medio.

---

38 http://europe-v-facebook.org/EN/Objectives/objectives.html

39 http://www.avaaz.org/es/community.php

40 https://www.change.org/impact

En 2014 se estrenaba en Sundance el documental The Internet's Own Boy: The Story of Aaron Swartz. Cofundador de Reddit, sitio web donde los usuarios pueden agregar y votar enlaces sobre contenidos web. Director técnico de Open Library, colaborador de la creación de Creative Commons y activista contra la ley SOPA[41], Swartz saltó a la fama mediática a raíz de la descarga gratuita de artículos especializados de la revista académica JSTOR, protegidos con Copyright.

JSTOR representa la mayor base de datos académicos existentes, pero su acceso está restringido a usuarios registrados y su uso en universidades y academias está sujeto a pago. Aaron Swartz, desde el MIT, se introdujo en los servidores de JSTOR y descargó, sin suscripción, miles de artículos protegidos por Copyright sin intención, en principio, de hacer un uso comercial de los mismos. Fue acusado de crímenes informáticos y se enfrentaba a una multa de 4 millones de dólares y una condena de más de 50 años de prisión. Ante esta presión y debido a la situación en la que se encontraba, Aaron Swartz fue hallado muerto por suicidio el 11 de enero de 2013.

Estos son sólo una pequeña muestra del ciberactivismo pero ponen de manifiesto una alternativa fundamental a la hora de abordar la libertad en el ciberespacio. Es la capacidad de este espacio social para unir a personas bajo un mismo paraguas que de otro modo resultaría complicado e incluso a veces imposible de reunir. Las revoluciones árabes conocidas como "primavera árabe" son un claro ejemplo del poder del ciberespacio para unir a ciudadanos y pueblos contra acciones, situaciones y gobiernos contrarios a los intereses generales de la población. Si bien es cierto que, en términos absolutos, no se puede hablar de una democracia y libertad en Internet, estos ejemplos ayudan a entender cómo se puede alcanzar ese objetivo, que tiene que ser común a todos los miembros de esta aldea global.

[41] Ley para estadounidense para parar la piratería online.

CAPÍTULO 3:
GOOGLE.
EL GIGANTE DE INTERNET

Es fácil asociar Internet con Google. “Hacerse un Google” o “Googlear” son expresiones del todo aceptadas dentro de la comunidad de internautas. Muchas veces incluso se habla de Internet refiriéndose a la empresa. De hecho, muchas de esas veces no es a la empresa sino al buscador al que se hace referencia para referirse a Internet. La página principal con sus letras de colores sobre fondo blanco es Internet.

Desde la aparición del motor de búsqueda Google y sus futuras creaciones, creaciones que se volverán, con el tiempo, habituales en la vida diaria de las personas, la forma de navegar por la red ha cambiado. No sólo el modo en que los usuarios “preguntan por algo” en Internet, se comunican o navegan. También ha cambiado la propia estructura de Internet: el modo en que se busca y presenta la información; la mercadotecnia; la publicidad y el comercio, en este espacio llamado comercio electrónico, etc. En general Google ha cambiado la forma de entender la red, esto es, el modo en que los usuarios se relacionan *con* y *en* la red.

Esto se debe a varios factores, dos de ellos clave para entender el aumento exponencial y continuo de usuarios de Google. Ahora, matizado y tamizado con el tiempo, Google ha dejado de ser lo que era; una empresa adorada por geeks del mundo entero que veían en ella, no sólo la que había entendido sus necesidades como usuarios sino la que les había ofrecido herramientas que jamás podrían haber soñado. Sus seguidores eran legión, el merchandasing de la empresa contiene casi cualquier objeto donde pueda aparecer el logotipo de la empresa, trabajar en Google significaba haber tocado techo en la carrera profesional y cualquiera hubiera hecho lo imposible por formar parte de la empresa multicolor.

3.1. Los primeros motores de búsqueda. Donde lo importante no es el usuario

Antes de la aparición en escena de Google, un período comprendido entre 1994 y 1996, el escenario en Internet era muy diferente. Las viejas empresas se lanzaron a Internet y muchas otras nacieron aprovechando el nuevo espacio creado. El número de usuarios iba creciendo, sus inquietudes, sus deseos y también sus exigencias aumentaban a medida que lo hacía la red. Nacía el boom de Internet. Pero en aquellos tiempos Internet no estaba hecha “a medida humana”. El usuario no era un actor del escenario cibernético. El diseño de los portales y los navegadores estaba destinado a maximizar las posibilidades de generar beneficios por cada visita y la experiencia del usuario no formaba parte de esa construcción.

Al principio de la era de Internet, los motores de búsqueda eran, en realidad, directorios, una recopilación de información en diversos formatos que era ofrecida al usuario de un modo más o menos ordenado. Estos directorios eran creados por personas que tenían por trabajo rastrear la red y ordenar la información de un modo relevante para ofrecérsela al usuario. La calidad de la información era buena pero la lentitud a la hora de actualizar los resultados dificultaba seguir manteniendo la red de ese modo. De ahí la aparición de "buscadores puros", aquellos que de un modo automático rastreaban y ordenaban la información, la indexaban en función de unas variables y la ofrecían al usuario en forma de respuesta.

De estos grandes almacenes de información destacaron en los primeros años de Internet Altavista, Yahoo!, Lycos, Infoseek y HotBot. La lista es más larga, y muchos directorios y motores de búsqueda aparecieron en aquellos años con mayor o menor éxito, como Excite, Webcrawler, Ask Jeeves o Northern Light. Pero aquéllos representan las diversas opciones que había en el mercado y muestran en su conjunto la necesidad que había de crear un solo producto que aunara de una forma eficiente lo mejor de cada una de esas empresas.

3.1.1. AltaVista

Creado a principios de 1995, AltaVista fue, durante mucho tiempo, el mejor y más usado buscador de Internet. En sus mejores momentos contaba con veinte millones de resultados y su sencillez y rapidez a la hora de devolver resultados le convertía en el preferido de los internautas. Su declive está absolutamente ligado al surgimiento y crecimiento de Google, sin que haya una causa mayor. Simplemente apareció una empresa que lo hacía mejor y más apetecible para el consumidor. Altavista era un espacio, dentro de la norma de aquel entonces, sencillo, ofrecía un servicio de traducción llamado Babel Fish así como la posibilidad de búsquedas de noticias, imágenes, audios y vídeos.

Altavista acabaría siendo absorbida por Overture (y ésta a su vez por Yahoo!), empresa pionera en la rentabilización de las búsquedas. Overture había creado un tipo de publicidad nueva, ahora llamada patrocinada. Cuando el usuario realizaba una búsqueda concreta Overture ofrecía como resultados anuncios publicitarios relacionados con esa búsqueda. Así mismo fue la impulsora del llamado pago por click o PPC por sus en inglés (pay-per-click). Este tipo de pago consiste en que el anunciante paga en función de los clicks que se hagan sobre su mensaje publicitario. En 2003

Yahoo! compra Altavista y AlltheWeb.com llevándose consigo no solo los millones de usuarios sino también la tecnología.

3.1.2. Yahoo!

Lanzado en 1994, Yahoo! fue en su momento el directorio más importante de la red. Su idea principal se basaba en la creencia que una máquina o algoritmo no podría sustituir a un humano a la hora de clasificar la información en Internet. Con el tiempo se vería que eso no era cierto. La historia de Yahoo! y Google es una historia tensa, donde se juntan los esfuerzos por luchar contra un enemigo común, Microsoft, y una férrea rivalidad cuando el enemigo deja de existir. Durante un período de cuatro años, comprendidos entre 2000 y 2004, los resultados de Yahoo! eran ofrecidos mediante la tecnología de Google hasta que el acuerdo se rompió. Para entonces, Yahoo! había perdido usuarios frente a la potente tecnología que ofrecía Google.

> Existe una gran diferencia en la historia, en ocasiones tan paralela, entre ambas compañías, y es la utilización de la tecnología. Google ha pensado cómo mejorar y facilitar la vida del usuario, mientras Yahoo! siempre pensó que el usuario ya estaba allí, que era secundario y un mero consumidor de publicidad.
> (Suárez, 2012, p. 85)

3.1.3. Lycos

Lycos (1995) supo ver entre toda la competencia que el éxito consistía en ser grande. Algo que tendrá en cuenta más tarde Google y que llevará esa misión como estandarte. Su idea principal era que cuanta más información disponible tuviera más se podría ofrecer al usuario, lo que se traduciría en tráfico en su buscador y esto en beneficios. En 1996 Lycos había multiplicado su indexación hasta situarse en cerca de sesenta millones de páginas web indexadas[42].

3.1.4. Infoseek

Infoseek, creada en 1994, comenzó con unas cuantas miles de páginas web. Su éxito radicó en el acuerdo que firmó con NetScape para convertirse en su buscador por defecto. Así, igual que pasara entre Yahoo! y Google, quien realizara una búsqueda desde Infoseek obtendría resultados de

[42] http://searchenginewatch.com/sew/news/2064656/happy-birthday-lycos

NetScape, navegador preferido de los noventa basado en el software libre y gratuito. Esta alianza supuso para Infoseek unas siete millones de visitas en 1997[43].

3.1.5. HotBot

Entre los primeros buscadores llamados puros, aquellos que sólo ofrecen búsquedas, estaba Hotbot. Este buscador mostraba los resultados por relevancia y los agrupaba por sitios. Además incluía la posibilidad de filtrar los resultados por fecha de modificación, idioma o tipo de contenido. Esto es, introdujo la acción de "refinar la búsqueda". El software utilizado para hacerlo era propiedad de Inktomi, empresa que sería comprada por Yahoo! en 2002 para hacer frente a la tecnología de Google.

3.2. Frankenstein Google. Cómo hacer un buscador con lo mejor de sus predecesores

Dentro de este escenario era difícil encontrar un buscador que reuniera todas estas facultades que, por separado, habían reunido el grupo de buscadores y directorios de aquellos primeros años. Aquellos que permitían una mejor búsqueda ofrecían menos resultados que aquellos que disponían de una mayor base de datos. Pero éstos a su vez carecían del software que permitía indexar rápida y constantemente la red, por lo que aun teniendo mucha información ésta se quedaba pronto desfasada.

Así mismo, tanto unas como otras, diseñaban sus motores de búsqueda sin tener en cuenta una parte esencial de las mismas, el consumidor final. El usuario, que finalmente era el que hacia uso de la herramienta no era tenido en cuenta en el diseño, tan solo en la medida de receptor de información y publicidad. De este modo, los primeros motores de búsqueda tenían una apariencia poco atractiva para el usuario, con muchos colores, formatos e información en sus páginas principales. La idea era que el usuario consumiera esa información e hiciera uso de ella generando así tráfico y por lo tanto ganancias al motor. "Antes de la irrupción de Google los buscadores no eran un gran negocio y no se invertía demasiado en su desarrollo. Se concebían como herramientas secundarias, no como un elemento clave del desarrollo de la web" (Suárez, 2012, p. 19).

Sería intrépido pensar que había un objetivo avasallador en la forma de hacer de los motores de búsqueda pioneros. Es más sensato afirmar que el mundo de Internet era un espacio por construir y no había modelos establecidos sobre cómo hacer las cosas. Es razonable pensar que se intentó

[43] http://web.archive.org/web/20090501140446/http://www.clubi.ie/webserch/engines/infoseek/history.htm

trasladar directamente el mundo de los negocios del espacio no cibernético al nuevo espacio digital. De este modo, los motores de búsqueda, que no eran otra cosa que tablones de anuncios, librerías, enciclopedias o páginas amarillas digitales, en la medida en que su objeto era la difusión de información, entendían que su página de presentación, cual índice, debía contener toda la información sobre qué y cómo hacer uso del motor.

> Aquellos portales eran un enorme cajón de sastre que incluía millones de páginas web mal interpretadas por los primeros robots de búsquedas que las almacenaban. Por eso no podían ofrecer al usuario respuestas correctas y concretas a sus cada vez más evolucionadas necesidades.
> (Suárez, 2012, p. 19).

Para un motor de búsqueda existen dos tipos de clientes, distinción que ya se encuentra en Castells, llamados usuarios. Están aquellas empresas que desean hacer negocios con el tráfico y consumo de los usuarios del motor de búsqueda, por medio de su aparición en los resultados de búsqueda, su posicionamiento en algún lugar determinado del buscador, mediante enlaces hacia su propia web, etc. Este tipo de cliente es aquel usuario que Castells denomina usuario-productor. Al mismo tiempo existe el usuario-consumidor, la persona individual que realiza búsquedas en Internet. Éste es también cliente del motor de búsqueda en la medida en que lo utiliza como buscador para realizar consultas.

De este modo, no haciendo distinción entre ambos tipos de clientes, las páginas principales de los motores de búsqueda estaban dirigidas a ambos por igual. Así, aquel usuario que deseaba realizar una consulta, tenía que encontrar la barra de búsqueda entre mensajes dirigidos a empresas, barras publicitarias, anuncios de empresas, fondos de pantalla coloridos y en definitiva un surtido conjunto lleno de contenido.

En resumen, al comienzo de Internet, los buscadores, perdidos en este nuevo entorno sin saber muy bien hacia donde dirigir sus esfuerzos, carecían de dos aspectos fundamentales que harían que Google arrasara con el mercado de los motores de búsqueda: un interés por el comportamiento del usuario a la hora de navegar por Internet y una buena, mucha, actualizada y sobre todo, ordenada información.

Google vino a cambiar todo eso. En 1997, después de varios años de trabajo, se estrena la versión beta del motor de búsqueda. En fondo blanco, con letras de colores de tipo infantil y con una barra de búsqueda central. Poco más había en la página principal del motor. Un espacio para la subscripción, que sería eliminada poco después, un espacio para especificar el número de resultados que se deseaba aparecieran y un espacio llamado "I'm feeling lucky".

Una sencillez que alejaba a Google del resto de motores de búsqueda y le acercaba al usuario. Sin más objeto que realizar una búsqueda, el usuario podía elegir hacerla de modo normal, donde los resultados aparecerían ordenados según las valoraciones de la propia red o en modo "I'm feeling lucky". En este caso el usuario era redirigido al primer resultado que apareciera en la clasificación del PageRank sin que apareciera una lista de resultados, de modo que, con suerte (de ahí el nombre) el usuario daría con la respuesta esperada sin tener que buscar más.

> Unlike a lot of other web pages, the Google home page was so sparse it looked unfinished. The page had a box to type in requests and two buttons underneath, one for search and another labeled I'm Feeling Lucky, a startling bid of confidence that implied that, unlike the competition, Google was capable of nailing your request on the first try.
> (Levy, 2011, p. 56).

La segunda cosa que marcaría la diferencia respecto a sus antecesores era la organización y la calidad de la información, y esto es algo que consiguieron con el PageRank. El PageRank y la fundación de Google es obra de dos estudiantes de ciencias de computación de Standford, Larry Page, de éste el nombre de PageRank, y Sergey Brin. El PageRank es un conjunto de algoritmos que permite clasificar mediante una valoración numérica la relevancia de una determinada información (documento, archivo, web, vídeo, audio y cualquier otro dato) para ofrecerla de una forma ordenada en función del valor que se le de en el ciberespacio. Este valor viene determinado, entre otras cosas, por los enlaces que un objeto informacional tenga en toda la red. Así, una web, por ejemplo, que sea enlazada por muchas otras tendrá un PageRank alto, este alto significa aparecer en los primeros puestos de los resultados de búsqueda.

Póngase un ejemplo. La enciclopedia colaborativa Wikipedia aparece como enlace en muchas páginas web para realizar búsquedas, además contiene mucha información y muy relevante. Así

mismo existen indicadores que advierten que los usuarios que son enlazados a esta enciclopedia no realizan más búsquedas, por lo que se entiende que el usuario ha conseguido en ella la información solicitada. El PageRank calcula entonces que éste es un buen resultado, o lo que es lo mismo, tiene mucha relevancia en Internet, lo que hace que deba aparecer en los primeros puestos de los resultados que ofrece Google. El PageRank, junto con la importancia de la experiencia del usuario, es lo que marca la diferencia respecto a otros buscadores.

> Aun sin saberlo, Page y Brin tenían ya en aquel momento inicial dos cosas que les hacían especiales. La primera, una idea basada en el análisis y el estudio de las necesidades y el comportamiento de los usuarios [...] La segunda, el desarrollo de un producto, el PageRank, que incluso en un estado muy básico e inicial era ya mucho más potente y adaptado a los tiempos que el de su competencia.
> (Suárez, 2012, p. 24)

La fórmula del algoritmo fue descrita en un documento que presentaba el prototipo de Google. Escrito por ambos fundadores y titulado *"The Anatomy of a Large-Scale Hypertextual Web Search Engine*", presentaban así Google:

> *We present Google, a prototype of a large-scale search engine which makes heavy use of the structure present in hypertext. Google is designed to crawl and index the Web efficiently and produce much more satisfying search results than existing systems.*
> (Brin and Page, 1998, p. 1)

En ambos aspectos radica la supremacía de Google en el mercado de los motores de búsqueda y por eso no es de extrañar que sea también un secreto guardado con mucho celo. El algoritmo fue presentado a patente en el mismo año 1997, un año antes de la presentación del documento antes mencionado, por lo que no se ha podido conocer nunca con exactitud su funcionamiento.

Si bien es cierto que el "PageRank is a Web page ranking technique that has been a fundamental ingredient in the development and success of the Google search engine" (Franceschet, 2010, p. 1) existen hoy en día muchas voces que disienten sobre la efectividad del ordenamiento de resultados ofrecidos por Google. Estudios como el de Elisabeth Van Couvering ponen de manifiesto que existen otros aspectos que también son relevantes para la calidad de los motores de búsqueda. "As a

result of search engine optimisation and spamming practices, it is not only search engine providers who determine the relevancy of the results" (Van Couvering, 2004, p. 24). Así mismo, investigaciones relacionadas con la actualización e indexación (inclusión en el "índice" de Internet una web o contenido determinado) afirman que existe un problema a la hora de abordar con rigor la importancia de la información ofrecida en un determinado momento por los motores de búsqueda. Entre éstos se encuentran los trabajos de Liewen Vaughan (2003 y 2011) y Paul Wouters, Lina Helsten y Loet Laydesdorff (2004 y 2006), entre otros.

Lawrence M. Hinman presenta así un artículo al respecto: "Search engines play an increasingly pivotal role in the distribution and eventual construction of knowledge, yet they are largely unnoticed, their procedures are opaque, and they are almost completely devoid of independent oversight" (Hinman, 2005, p. 19). Desde otro punto de vista, Tobias Blanke trata el tema de la relevancia de los motores de búsqueda desde el aspecto de la simulación de la interpretación humana.

> [...] the ethical problems of search engines do not begin with the fact that they decide about relevance but with how they decide about it. The technology has been developed so as to decide itself. Its decision is supposed to reveal the meaning in the data and simulate information. How is this meaning retrieval done? The first thing to notice is that it is always limited by the 'objective mind' of a machine. A search engine is designed to retrieve information relevant to a human's subjective situation.
> (Blanke, 2005, p. 36)

Guste ahora o no, al menos en los primeros años de este siglo, Google era el mejor y más valorado motor de búsqueda del mercado. A finales de 1999, un año después de su puesta en marcha, Google contaba con alrededor de siete millones de visitas diarias (Suárez, 2012, p. 32). Visitas que por otra parte no generaban beneficios. La preocupación por la experiencia del usuario significaba no poder incluir en los resultados banners, pop ups ni otro tipo de publicidad que alterara el aspecto de su página. El banner o banderola es un tipo de publicidad en Internet que tiene como objetivo dirigir la atención del usuario hacia él, muchas veces alejado del diseño original del sitio web en el que se encuentra, haciendo que destaque sobre él. Las pop up o ventanas emergentes tienen el mismo objetivo que los banners con la diferencia de que son ventanas que aparecen automáticamente sobre la web en la que el usuario está y que deben ser cerradas para que desaparezcan.

Ambas formas de publicidad están alejadas de lo que Google consideraba una buena experiencia del usuario. Por eso en el año 2000 Google decide incluir un tipo de publicidad no invasiva y siempre relacionada con la búsqueda del usuario, creando así Adwords. Ese mismo año Google firma varios acuerdos con otros motores de búsqueda para que éstos ofrezcan sus resultados. Así Google amplia su tráfico con empresas como Yahoo!, NetEase en China y BiGlobe en Japón, Lycos en Corea y UOL en América Latina. A medida que los usuarios fueron conscientes de que los resultados de estas empresas eran ofrecidos por Google, pronto comenzaron a utilizar el buscador como fuente principal de información (Suárez, 2012, p. 35). Ya no era necesario pasar por Yahoo!, NetEase, BiGlobe o Lycos si la respuesta la tenía Google.

Poco a poco Google fue incluyendo elementos de sus predecesores. Así, fue añadiendo idiomas para realizar las búsquedas, como haría en su momento AltaVista. También incluyó noticias con su GoogleNews, hecho que le traería más de un problema a la empresa. La Agence France-Presse (AFP) demandó a Google en marzo de 2005 por violación de derechos de autor al utilizar fotos, vídeos y artículos de la AFP sin su autorización. El caso fue cerrado bajo acuerdo en 2007 (Suárez, 2012, p. 133-134).

Se creó Google Images y Google Video. Este último proyecto no llegó a dar sus frutos debido a que ya existía YouTube. La decisión de Google fue tajante al respecto y desembocó en la compra en 2006 de la plataforma por 1650 millones de dólares[44]. La indexación, que comenzara Lycos como su mayor aporte al mundo de los motores de búsqueda, fue superada con éxito por el PageRank, así como la relevancia y el refinamiento de búsqueda de Hotbot. El acuerdo de Infoseek con Netscape de aparecer como buscador principal fue el ejemplo que siguió Google al firmar los acuerdos con Yahoo! en 2002 y con Firefox en 2004.

El éxito de Google no fue tan sólo cuestión de incluir en su motor lo mejor de cada uno de los motores anteriores. Google fue añadiendo nuevos servicios que fueran atractivos para el consumidor, esto es, que aumentaran de forma positiva la experiencia del usuario, y algo importante para éste, que siempre parecieran gratuitos. Además de noticias, vídeos, idiomas, bots[45] que valoran e indexan webs por billones, Google ha ampliado su oferta con nuevos productos.

---

[44] http://tecnologia.elpais.com/tecnologia/2006/10/09/actualidad/1160382485_850215.html

[45] El robot de Google es el medio de rastreo por el cual el motor de búsqueda descubre, actualiza y añade al índice páginas nuevas.

Así, ha incluido un servicio de correo electrónico, conocido por Gmail, que comenzó a funcionar en 2004. Con una capacidad de 7GB de almacenamiento, al principio sólo se podía acceder con una invitación de un usuario. Esto hizo que los internautas desearan, aun más, tener una cuenta propia.

> En medio de una intensa campaña de marketing viral, las invitaciones llegaron a subastarse por cientos de dólares [...] Mientras tanto, los hasta entonces grandes proveedores de correo electrónico, como el servicio Hotmail de Microsoft, Yahoo! o AOL, limitaban la capacidad de almacenamiento de los usuarios, aumentaban la publicidad intrusiva y no ofrecían opciones realmente útiles, ya que estaban empeñados en rentabilizar cuanto antes sus servicios. Podemos decir que el sector estaba estancado, y fue en aquel momento cuando Google lanzó el correo que todos soñábamos tener. (Suárez, 2012, p. 50)

En 2008 aparecía el navegador Google Chrome, que debido a su sencillez, rapidez y estabilidad se convertía en 2011 en el tercer navegador más utilizado, después de Internet Explorer y de Firefox y adelantaba a ambos en 2015 con el doble de usuarios. Mientras Internet Explorer y Firefox contaban en octubre de ese año con el 15,38% y el 15,53% de los usuarios respectivamente, Google Chrome se hacía con el 53,62% de los usuarios de Internet[46].

Con la adquisición de Android, un sistema operativo para dispositivos móviles, Google se hacía también con el mercado de la telefonía e Internet móvil. Actualmente Android es el sistema operativo para dispositivos móviles más usado del planeta, por delante de Windows Phone e IOS (sistema operativo para dispositivos móviles de Apple) juntos[47].

Cuenta así mismo con un alojamiento de archivos en la nube, llamado en un primer momento Google Docs y que 2012 pasó a llamarse Google Drive. Este servicio permite almacenar de forma gratuita hasta 15 gigabytes de información, pudiendo ampliarse con una subscripción de pago. Además de alojamiento web, ofrece la posibilidad de editar hojas de cálculo, textos y presentaciones así como la creación de dibujos, entre otras opciones. Así mismo permite la

---

46 http://gs.statcounter.com/

47 http://www.ibtimes.com/android-vs-ios-whats-most-popular-mobile-operating-system-your-country-1464892

modificación de archivos sin una conexión a Internet. Puede sincronizarse con otros productos Google como Gmail o Picasa, de modo que se pueden guardar fotos o correos electrónicos.

Llegó también el momento de hacerse con el mercado de las redes sociales creando para ello Google+, plataforma lanzada en 2011 en un intento de competir en el mercado de las redes sociales. Este servicio es el producto de otros intentos de la compañía por entrar en el mundo de las redes sociales. Desde Orkut, creada en 2004 y mantenida hasta 2014 hasta Google Buzz, con su salida al mercado en 2010 e integrada en su servicio de correo electrónico Gmail y cerrada un año más tarde.

El sistema de relaciones de Google+ se basa en círculos. Los usuarios pueden crear círculos de amigos de modo que aquellos que están en un círculo de amigos no tienen acceso a otros círculos donde no estén incluidos, aunque sí pueden ver los nombres de las personas que el usuario tenga como amigos. Cuenta así mismo con una función de comunidades, en las que el usuario puede compartir determinada información con aquellos usuarios que estén dentro de esa comunidad, compañeros de trabajo, amigos de la infancia, familia, etc. Existe una confianza generalizada entre los usuarios en los productos y servicios que lanza Google. Cada novedad lanzada por la compañía tiene una respuesta inmediata por parte de los usuarios, con independencia del futuro del producto. Google+ no es una excepción. En tres semanas desde su lanzamiento Google+ había sumado 20 millones de usuarios[48] y en un día pasó a ser la aplicación gratuita más popular en la App Store de Apple[49].

La compañía cuenta con más servicios como Google Earth, Google Académico, Google Maps y Google Street View, Google Shopping o Google Calendar. La empresa Alphabet Inc. ha conseguido llegar a millones de usuarios de diversas formas y tiene representación en casi cualquier cosa que sucede en la red.

Los servicios antes mencionados estarían dirigidos a los consumidores/usuarios mientras que los que se muestran ahora lo están a los productores/usuarios. Esta afirmación hay que atenderla con matices, ya que muchas veces ambos tipos de usuarios se confunden y se solapan. Los productores/usuarios utilizan muchos de los servicios que Google ofrece a los consumidores/usuarios y éstos a

---

48 http://www.cnet.com/news/google-hits-20-million-mark-in-three-weeks/

49 http://techcrunch.com/2011/07/20/google-now-the-top-free-app-in-the-apple-app-store/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29

su vez hacen uso de otros productos. Lo que se intenta afirmar es que un consumidor/usuario, a no ser que en algún momento sea un productor/usuario, por ejemplo una persona que tenga algún servicio o producto en la red ya sea un blog, una página web personal, algún negocio en Internet, etc., no hará uso de los servicios que se muestran a continuación, dirigidos en exclusiva a productores/usuarios.

Adwords es el programa de Google que ofrece publicidad patrocinada en sus resultados. Mediante el pago por clic los anunciantes pagan a Google cuando un usuario realiza un clic sobre el anuncio. El precio que se paga por cada clic no es estable sino que depende de una subasta en función de la oferta y la demanda de cada sector o palabra. Con la introducción de este programa Google dejó de lado lo que había sido su marca identitaria que se definía por no ofrecer publicidad a los usuarios. Algo fundamental para el usuario-consumidor es que la publicidad ofrecida no es invasiva sino que se integra dentro de los resultados de búsqueda del usuario.

Adwords funciona en colaboración con Adsense. Esto es una serie de herramientas que realizan el posicionamiento y resultado de los anuncios comprados por las empresas en Adwords. Adsense no es una creación pionera de Google. En 1998 se creaba la empresa Oingo Inc. que aportó a Internet un algoritmo basado en palabras y que sería comprada por Google en 2003[50]. Adsense permite introducir publicidad en las diferentes página web. Así, si se tiene una página web de restaurantes, el editor de la página puede, mediante Adsense, añadir publicidad relacionada con la restauración. El precio del anuncio se fija mediante una subasta a tiempo real del espacio publicitario en función de variables como la importancia de la página web, el tamaño o posición del anuncio en la página web o el tráfico que genere esa página.

DoubleClick ofrece servicios a empresas para que puedan gestionar su publicidad online. Así mismo produce informes sobre el movimiento y el rendimiento de cada uno de los anuncios que una empresa o negocio tenga. Del mismo modo que Adsense, DoubleClick fue comprada en 2008 por Google, no sin antes pasar por la Comisión Federal de Comercio de los Estados Unidos debido a una sospecha de monopolio de publicidad online, hecho iniciado una denuncia de Microsoft[51].

---

[50] http://googlepress.blogspot.com.es/2004/04/google-acquires-applied-semantics.html

[51] http://www.reuters.com/article/2007/12/20/us-doubleclick-google-idUSN2039512220071220

AdMob es para los dispositivos móviles lo que Adsense para los ordenadores. AdMob ofrece publicidad dentro de las aplicaciones en forma de banner. Esta incluye en sus modelos de pago por publicidad el llamado pay-per-call o pago por llamada, donde el anunciante paga en función de las llamadas que reciba de posibles clientes a través del anuncio publicado en una aplicación móvil.

Por su parte, Google Analytics es una herramienta que ofrece información sobre el tráfico de una página web. Con ésta, el administrador de una página web puede obtener información relativa a las visitas diarias, desde qué tipo de dispositivo se realiza la consulta, desde qué posición geográfica se ha realizado la entrada, cuánto tiempo se ha estado en la web, cuánto tiempo se ha estado en la web en función de la posición geográfica, qué red social y cómo ha influido en el tráfico de la web esa red social, qué compras y tipo de transacción se ha realizado, cómo ha llegado el visitante de la página, esto es, ver los pasos que ha seguido para llegar hasta la web, de modo que se pueda optimizar la publicidad introduciéndola en los "caminos" más utilizados hasta una web en concreto y un largo etcétera de personalización del servicio[52].

En resumen, con Adwords Google ofrece publicidad en los resultados de búsqueda, resultados que están organizados en función del PageRank. Con Adsense permite la inclusión de publicidad en las diferentes páginas web con un precio marcado, entre otras cosas, por su herramienta de análisis Google Analytics. Con ésta, controla, en tanto que conoce, el valor (el tráfico) de cada una de las páginas web de la red, pudiendo de este modo marcar un precio de mercado de la publicidad en línea en función de esa información.

[52] https://www.google.es/intl/es_ALL/analytics/features/index.html

CAPÍTULO 4:
PRIVACIDAD EN EL CIBERESPACIO

4.1. Privacidad de la información o privacidad informacional

En el capítulo dedicado a la sociología en el ciberespacio se ha señalado que en éste, todo lo que sucede tiene carácter informacional. Echeverría contraponía la informacionalidad del tercer entorno frente a la materialidad de los entornos previos. Castells denomina al nuevo paradigma que suponen las tecnologías digitales informacionalismo. La privacidad, por lo tanto, no se separa de esa supremacía de lo informacional y se entenderá entonces como privacidad de la información.

Según Johnson, "entre todas las preocupaciones sociales y éticas relacionadas con el uso de los ordenadores, la primera que probablemente llamó la atención pública fue el mantenimiento de archivos automatizados con datos relativos a la vida privada de las personas" (Johnson, 1996, p. 111). La Stanford Enclycopedia of Philosophy remarca esa primera preocupación por la privacidad señalando que: "one of the earliest computer ethics topics to arose public interest was privacy"[53]. En su artículo *Towards a Theory of privacy in the Information Age*, James H. Moor comienza su artículo afirmando algo similar: "when we think of ethical problems involving computing probably none us more paradigmatic than the issue of privacy" (Moor, 1997, p. 27).

A día de hoy es posible afirmar, como se ha visto en la páginas precedentes, que la privacidad sigue siendo uno de los temas centrales de la ciberética y una preocupación para cibernautas, instituciones, empresas y gobiernos, así como para filósofos, pensadores y profesionales de las ciencias informáticas. Si bien es cierto que cada uno de estos agentes se enfrenta al tema desde un punto de vista diferente todos comparten la perspectiva de que ésta es clave para la gobernabilidad del ciberespacio.

La Real Academia Española define la *privacidad* como "el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión y lo *privado* se refiere a lo que se ejecuta a la vista de pocos, familiar y domésticamente, sin formalidad ni ceremonia"[54]. Con las tecnologías digitales y su capacidad de recopilar, procesar, almacenar, recombinar y disponer de datos, la privacidad se ha volcado hacia la información.

> Philosophers, like everyone, have been struck by the broad dissemination and the forceful impact of information techonology during the last few decades. Therefore, it

[53] http://plato.stanford.edu/entries/ethics-computer/

[54] http://dle.rae.es/?id=UD4g0KW y http://dle.rae.es/?id=UD9ciF2lUDCTc5q

> is not surprising that most contemporary philosophical accounts of privacy tie it closely to the concept of information.
> (Moor, 1990, p. 74)

De este modo, al tratar en esta investigación la privacidad desde la perspectiva de la ciberética, ésta debe entenderse como privacidad de la información. Este hecho es significativo ya que ha transformado y ampliado de una manera notable el concepto mismo de privacidad y lo privado. Hasta la entrada de las tecnologías digitales como medio fundamental de comunicación estos conceptos se entendían como relativos a la vida privada, a los quehaceres que se tenían como íntimos y distintos a la vida pública y a lo público, distinción que, por otra parte, ya se encuentra en la *Política* de Aristóteles al hablar de *oikos* y *polis* como conceptos contrapuestos.

La familia, el domicilio o la correspondencia eran vistos como aspectos de aquello privado que había que salvaguardar, como sostiene el artículo 12 de la Declaración Universal de los Derechos Humanos[55]. Hoy en día esa información tenida como privada resulta insuficiente a la hora de hablar de privacidad. El amplio acceso a ese tipo de información, así como la propia exposición que los individuos hacen de esa parte de sus vidas en el ciberespacio, es suficiente para ver cómo la privacidad es algo que no puede reducirse a meros datos personales.

Un ejemplo de esto son las redes sociales. En ellas los individuos pueden poner su lugar de nacimiento, su lugar de residencia, el estado civil, su orientación sexual, sus hábitos y filias. Todos estos datos son expuestos por los propios cibernautas sin que ellos mismos lo consideren una violación de su privacidad, de su intimidad o su vida privada. La privacidad entendida como datos relativos a la vida privada es demasiado intimista para entender el concepto de privacidad en el ciberespacio. Es por esto que "the variety of privacy-related issues generated by computer technology has led philosophers and other thinkers to re-examine the concept of privacy itself" [56].

4.2. El valor de la privacidad

A medida que las tecnologías digitales avanzan y por avance se entiende que aumentan su capacidad de almacenar, gestionar y recombinar información, crece al mismo tiempo y de manera exponencial la preocupación de cibernautas y organismos por esa accesibilidad de la información.

---

[55] http://www.un.org/es/documents/udhr/

[56] http://plato.stanford.edu/archives/win2008/entries/ethics-computer/

Parte de los pensadores y filósofos interesados en las tecnologías digitales ven la privacidad en términos de control o acceso a la información. Antes de desarrollar las diversas teorías sobre el concepto de privacidad se debe hacer un apunte sobre el valor que se le otorga a la privacidad que conllevará una determinada teoría o posición al respecto.

4.2.1. Valor intrínseco y valor instrumental

Se dice de una acción, una cosa o estado de cosas que puede tener dos tipos de valor principalmente (por cuestiones prácticas y de argumentación no se hará referencia al valor originador y valor contributivo que apunta por ejemplo R. Nozick, [1983]). Así, se dice que algo tiene valor intrínseco cuando se considera bueno o deseable por sí mismo. Por el contrario, se dice que algo tiene valor instrumental cuando permite alcanzar un fin o propósito.

> Nuestra propia felicidad, por ejemplo, tiene valor intrínseco, al menos para la mayoría de nosotros, en el sentido de que la deseamos por sí misma. El dinero, por otra parte, tiene solo un valor instrumental para nosotros. Lo queremos por las cosas que podemos comprar con él, pero si naufragáramos en una isla desierta, no lo querríamos (mientras que la felicidad sería tan importante para nosotros en una isla desierta como en cualquier otro sitio).
> (Singer, 1995, p. 275)

En torno a la privacidad y a su importancia para el debate ético en el ciberespacio surge la cuestión de si ésta tiene un valor intrínseco o si por el contrario tiene un valor meramente instrumental. Esto significa preguntarse si la privacidad debe protegerse y perseguirse como un fin o es tan sólo un medio para conseguir un propósito. El valor dado a la privacidad será determinante para buscar y adoptar una postura concreta a la hora de entender y defender la privacidad.

Existe una tendencia en la literatura de la ciberética a entender la privacidad como un valor instrumental. “These instrumental justifications of privacy are the overwhelming philosophical favorites and may be adequate to ground the moral notion of privacy” (Moor, 1990, p. 81). Así, Stanley Benn entiende la privacidad como necesaria para crear relaciones de respeto entre las personas. “To respect someone as a person is to concede that one ought to take account of the way in which his enterprise might be affected by one’s own decisions*”* (Benn, 1984, p. 229). Por su parte, Charles Fried sostiene que la privacidad tiene un valor instrumental como medio para

desarrollar el amor, la amistad y la confianza. Ésta "necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust... without privacy they are simply inconceivable" (Fried, 1968, p. 477).

Tanto Benn como Fried parecen afirmar que la privacidad es necesaria para alcanzar un tipo de relaciones, ya sean de respeto, de amor o fraternidad. Esta variedad de relaciones es lo que lleva a James Rachels a proponer que la privacidad es necesaria, precisamente, para el desarrollo de las diversas relaciones sociales. Es el elemento privado lo que distingue las relaciones laborales de las amistosas, familiares o románticas:

> I want now to give an account of the value of privacy based on the idea that there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people. According to this account, privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have, and that is why it is important to us.
> (Rachels, 1975, p. 324)

Una propuesta que se puede encontrar a medio camino entre entender la privacidad como un valor instrumental y un valor intrínseco es la propuesta por Deborah Johnson (1996). Para ella, la privacidad es fundamental para entender la autonomía. Siguiendo como modelo la teoría kantiana afirma que la autonomía no puede entenderse sin la intimidad. De este modo, "la intimidad [que la autora utiliza como sinónimo de privacidad] se entiende no como un medio para conseguir la autonomía, el respeto o la democracia, sino una parte del significado de estos términos*"* (Jonhson, 1996, p. 119). Con este argumento se podría entender que, efectivamente, la privacidad tiene un valor intrínseco en la medida es que es condición necesaria para la autonomía. No es un medio para conseguirla sino, al contrario, es parte fundamental de la misma y por lo tanto, deseable en sus propios términos.

Ahora bien, como señala James Moor (1990) es posible concebir la autonomía sin privacidad. Téngase como ejercicio mental el guión de la película *El show de Truman.* Como se recordará Truman es, sin saberlo, el protagonista de un programa televisivo donde le observan, desde su nacimiento, miles de personas en todo el mundo. Es monitorizado y vigilado en un escenario

absoluto, donde toda su vida se genera en un gran plató de televisión. Vive su vida de un modo independiente donde las decisiones que toma son autónomas. De hecho, esa autonomía e independencia son las que le permiten finalmente descubrir que su vida ha sido un espectáculo televisivo. Este ejemplo, aunque de ficción, permite situarse ante la circunstancia de vivir sin privacidad pero con autonomía. Tanto el espectador del programa como el espectador de la película empatizan con Truman, desean que se de cuenta de lo que está viviendo y sea capaz de escapar de esa ficción. Este hecho pone de manifiesto que la privacidad se tiene con un valor que no puede reducirse a simple autonomía. Debe ser algo más que lleve al ser humano a buscarla y respetarla, por encima de la simple independencia de acción.

Podría afirmarse que la privacidad es una cuestión cultural y que existen sociedades en las que ésta tiene poca importancia o es entendida en otros términos. Incluso en la propia cultura occidental la intimidad y privacidad, como se entienden hoy en día, es una concepción relativamente nueva. Como hace notar el antropólogo Carmelo Lisón Tolosana, no será hasta la Edad Moderna donde la privacidad individual, dentro del núcleo familiar, haga su aparición. Hasta entonces,

> [...] frecuentemente toda la familia dormía en una sola habitación y era excepcional el que una cama estuviese ocupada por una sola persona [...] ya anochecido, tal vez podía acudir alguno de los mozos cortejadores de las mozas de la casa y se le permitía tumbarse sobre la paja y mantener una relación familiar con la moza cortejada a lo largo de la noche.
> (Lisón, 2007, p. 533)

James Moor intenta soslayar este relativismo cultural a través del concepto de *core values*. Por valores fundamentales considera las ideas de felicidad, vida, libertad, conocimiento, habilidad, recursos o seguridad. Para él, todas las sociedades, con independencia de sus rasgos culturales, valoran estos aspectos y son fundamentales para la supervivencia de la propia cultura. Así, el conocimiento es esencial para la perpetuación y el relevo generacional y cultural. La privacidad no forma parte de esos valores fundamentales, o dicho de otro modo, no es necesaria para la cultura. Sin embargo, sí lo es la seguridad, que podría tenerse como una forma de privacidad.

> Although privacy is not a core value per se, it is the expression of a core value, viz., the value of security [...] Moreover, because privacy is an expression of the core value

> of security, it is a plausible candidate for an intrinsic good in the context of a highly populated, computerized society.
> (Moor, 1997, p. 29)

Dicho esto cabe preguntarse sobre qué es la privacidad en el ciberespacio y, más concretamente, cómo puede protegerse la privacidad teniendo ésta como información. La respuesta más intuitiva podría afirmar que el medio más seguro para mantener la información alejada de las miradas indiscretas y ajenas sería no hacerla disponible en el ciberespacio. Aquellas personas que deseen mantener su privacidad deben alejarse de Internet y no hacer uso de aparatos electrónicos conectados a la red.

Pero esta respuesta elude e ignora la realidad de las redes telemáticas. No se trata, únicamente, de proteger la intimidad de las personas que chatean en los blogs o que se relacionan en las redes sociales. El ciberespacio está compuesto de bases de datos de todo tipo. La información médica de las personas; sus hábitos de consumo de las empresas donde realizan las compras; las transacciones bancarias en todas sus variantes, léase, el salario de las personas, el número de veces que se hace uso de las tarjetas de banco, a qué hora, en qué lugar, con qué motivo; los expedientes académicos de los estudiantes; y un largo etcétera. Con independencia del uso individual o personal que se haga de Internet y el ciberespacio, se recolecta información sobre cada ciudadano y cada individuo ya que "Information about us can be collected subtlety when we don't realize it. The greasing of information allows other computers to capture and manipulate information in ways we do not expect" (Moor, 1997, p. 27).

4.3. Privacidad como control de la información

Visto que la información es fundamental a la hora de hablar de privacidad en el ciberespacio, una pregunta pertinente es ¿cómo se entiende la privacidad en términos de información? Debido a que "tecnológicamente, la difusión de la información se puede realizar con o sin la autorización de la persona a la que afecta esta información, y puede realizarse tanto de forma deliberada como involuntaria" (Johnson, 1996, p. 115) parte del debate sobre la privacidad se realiza en términos de acceso. A grandes rasgos, que ahora se ampliarán, la idea principal es que cuanto menos acceso a la información se tenga de más privacidad se disfrutará y a la inversa, cuanto más acceso menos privacidad.

De este modo entiende Charles Fried la privacidad al afirmar que "Privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves" (Fried, 1984, p. 209). En la misma línea que Fried se encuentra Alan Westin cuando propone como definición de privacidad "the claim that individuals and groups determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1968, p. 200). Desde esta línea de pensamiento se sostiene que la privacidad es la capacidad de controlar, por parte de los individuos, la información que puede estar disponible para otras personas.

Sin embargo, este argumento, siguiendo el razonamiento de James Moor (1990), no resuelve el problema de la privacidad, en la medida en que se pueden encontrar situaciones en las que los individuos no tengan control sobre su información personal pero que no pierdan privacidad. Un ejemplo claro es el de los datos relativos a la salud de los pacientes. Cuando una persona acude al médico éste dispone de información privada del paciente. Al ser derivado a un especialista o al cambiar de profesional los datos sobre la salud del paciente son transmitidos al nuevo médico sin que el interesado tenga ningún control sobre el movimiento de esa información. Sucede entonces que ese traspaso y des-control por parte del paciente de su información personal no conlleva en sí misma una pérdida de privacidad ya que se entiende que esa distribución de información personal es necesaria para hacer el seguimiento del caso médico. De este modo, aunque se puede (y se debe) afirmar que la privacidad tiene que ver con cierto control sobre la información, no se puede ratificar que aquélla tenga que ver en su totalidad con el simple control sobre ésta. "If the information in these databases is properly used or, even more clearly, not used at all, the privacy is not diminished by the simple lack of control over that information" (Moor, 1990, p. 75).

El control de la información no puede, por lo tanto, ser definitorio para la privacidad, o dicho de otro modo, no puede ser su único componente Su importancia debe radicar en otro u otros aspectos que no sean el simple hecho de acceder a información confidencial o privada. Si bien es cierto que este acceso puede suponer una violación de la privacidad y por lo tanto debe ser importante para la misma, también es cierto, como se ha visto más arriba, que ese mismo acceso a la información puede mantener intacta la privacidad de la persona relativa a la información dada u obtenida. Existe, sin embargo, un desarrollo de la teoría de la privacidad como acceso que afirma que ésta no tiene que ver con el simple control del acceso a la información sino con un acceso restringido a dicha información.

4.4. Privacidad como acceso restringido a la información

Se ha visto que el acceso a determinada información es insuficiente a la hora de determinar si se posee, respeta o vulnera la privacidad. El modo de protegerla debe residir en algo más que la simple posibilidad de acceder a información. Como el ejemplo precedente mostraba, el hecho que un profesional médico tenga acceso a información relativa a la salud de un paciente no involucra la pérdida de su privacidad. Algo distinto sería, y ahí se podría hablar de pérdida, si todo el personal del centro sanitario, bedeles, personal de limpieza, administrativos, etc. tuviera acceso a esa información. En este caso, se podría considerar que el paciente está perdiendo cierto grado de privacidad, aunque cabría seguir preguntándose por lo motivos que llevan a que todo ese personal conozca determinada información. Podría resultar necesario que ese personal tuviera acceso a información sobre a la salud de un paciente para poder atenderle adecuadamente. Por estos motivos, algunas voces afirman que la privacidad depende de un acceso restringido a la información.

La idea principal sobre el acceso restringido afirma que la privacidad consiste en el control sobre qué personas o entes tienen acceso a qué información y en qué circunstancias. Efectivamente, estas variables acotan el acceso. De este modo argumenta Ruth Gavison al hablar sobre la privacidad como acceso restringido,

> Our interest in privacy, I argue, is related to our concern over our accessibility to others: the entent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are subject of others' attention. (Gavison, 1980, p 423)

Siguiendo el argumento (p. 426) sostiene que la definición de privacidad como control debe ser desestimada. El problema, afirma, es la escasa fuerza descriptiva del concepto de control ya que éste puede llevar al mismo tiempo tanto a una pérdida de privacidad como a su protección. Compartir algún asunto confidencial, por ejemplo, mantiene el control en la medida en que es la propia persona que decide hacer pública determinada cuestión. Pero también significa la pérdida de privacidad en la medida en que no es posible asegurar o controlar la diseminación de esa información por parte de las personas con las que se hay compartido. A pesar de esta afirmación, la autora continúa sobre el argumento del control de la información como privacidad:

> We need a framework within which privacy may be the result of a specific exercise of control, as when X decides not to disclose certain information about himself, or the result of something imposed on an individual against his wish, as when law prohibits the performance of sexual intercourse in a public place.
> (Gavison, 1980, p. 427)

La privacidad no es entonces un mero control sobre la información sino algo resultante de la limitación impuesta sobre el acceso a la información.“Privacy is a limitation of others’ access to an individual” donde la privacidad perfecta surge de la inaccesibilidad total a un individuo. Esta perfección de la privacidad se puede desarrollar de tres modos independientes pero relacionados: a través del secretismo, “in perfect privacy no one has any information about X”; a través del anonimato, “no one pays attention to X”; y a través de la soledad, “no one has physical access to X” (Gavison, 1980, p. 428-429).

En la vida en sociedad es evidente que esta privacidad perfecta es impracticable y que no es posible mantener en todo momento el secretismo, el anonimato y la soledad. Sin embargo, estos tres conceptos ayudan a entender el alcance y los presupuestos en los que se basa la idea del acceso restringido. El control es insuficiente para asegurar la privacidad de los individuos del mismo modo que lo es el acceso. Para que la privacidad sea efectiva tiene que existir, al menos, una restricción o limitación a ese acceso.

Otra autora que defiende la privacidad como acceso restringido es Anita Allen. Para ella, este tipo de privacidad se explica como “cierto grado de inaccesibilidad de las personas, sus estados mentales e información sobre ellas a los sentidos y la vigilancia de otras personas*”* (Allen, 1988, p. 34). Entiende que, como Gavison, la seclusión, la soledad, el secretismo, la confidencialidad y el anonimato son formas de privacidad. Así mismo, distingue dos tipos de privacidad como acceso restringido. La primera es aquella que tiene que ver con la información personal o de otras personas. La segunda deriva de la distinción entre público y privado. En este sentido entiende el acceso restringido como la falta de coacción ante la toma de decisiones, ya sea una injerencia ejercida por el gobierno o por otras personas.

Defendiendo que la privacidad en sí misma no es ni moralmente buena ni reprochable, aboga por una privacidad extensiva cuando se habla sobre la privacidad de las mujeres. En el caso de éstas,

enfatiza, hay que tener cuidado a la hora de tratar el tema de la privacidad ya que ésta puede significar un problema ante el abuso o una vulneración de sus derechos. Póngase el ejemplo de una mujer maltratada. La defensa de la privacidad en asuntos familiares puede ir en detrimento de la protección de la mujer ante una situación de abuso, en la medida en que una defensa radical de la privacidad familiar puede llevar a la situación de no poder intervenir en asuntos de maltrato por considerarse una falta de respeto de la privacidad de la vida familiar. Por otra parte, si se estima que las cuestiones relativas al núcleo familiar deben ser un asunto público, se podrían dar situaciones en las que los derechos de las mujeres se vulneran, en casos como, por ejemplo, el derecho a la interrupción de embarazos no deseados o la decisión de tomar medidas para su prevención. En ambos casos, un exceso de privacidad, ya sea protegiéndola o vulnerándola puede tener consecuencias negativas para las mujeres.

4.6. Privacidad como acceso restringido y controlado a la información

James Moor (1990) propone un tipo de acceso restringido más acotado haciendo énfasis en el concepto de situación. En su opinión "an individual or group has privacy in a situation if and only if in that situation the individual or group or information related to the individual or group is protected from the intrusion, obervation, and surveillance by others*"* (Moor, 1990 p. 76).

Afirma la existencia de dos tipos de situaciones privadas. Por un lado están aquellas que son naturalmente privadas y por otro las que lo son normativamente. Por situaciones naturalmente privadas entiende aquellas en la que las personas, con motivo de la situación en la que se encuentran, están protegidas de la intrusión de otros. Tómese el ejemplo de una persona que se encuentra en un lugar aislado o remoto, como puede ser una cueva o lo alto de una montaña con una flora espesa. No siendo este un contexto donde se espere encontrar a nadie alrededor se puede entender que aquí una persona disfruta de una privacidad natural. Por otra parte al no ser un espacio cerrado y particular sino abierto y público, si dentro de la cueva o en lo alto de la montaña aparece otra persona, automáticamente la privacidad se pierde. Ahora bien, en este caso no ser podría hablar, afirma el autor, de una pérdida de la misma, precisamente por ser un espacio abierto y público.

Por privacidad normativa entiende que, aun pudiendo ser natural, su fuerza reside en la ley o en la moral. En estas situaciones las personas están legal o moralmente sujetas a respetar la privacidad de un individuo. Imagínese una persona que está en su casa realizando una actividad cualquier. Ésta

goza de una privacidad natural en la medida en que el propio espacio cerrado hace de barrera para la intrusión de otras personas (las paredes de la casa constituyen aquí una barrera natural en tanto material) al tiempo que disfruta de una privacidad normativa, esto es, el espacio normativamente privado que es su casa. Tomando el ejemplo que utiliza el propio autor, enviar una carta en un sobre cerrado conlleva una privacidad natural, el sobre hace de barrera natural contra la intromisión al tiempo que cuenta con una privacidad normativa que dicta que no se lee el correo personal ajeno. En este caso, si otra persona se introdujera en su casa o mirase por la ventana para observar la actividad que está realizando el individuo entonces se estaría perdiendo y violando el derecho a su privacidad. Para Moor, esta distinción entre ambos tipos de situaciones es imprescindible a la hora de defender la privacidad como acceso restringido. "With different zones of privacy one can decide how much personal information to keep private and how much to make public" (Moor, 1997, p. 30).

La pregunta que se plantea a continuación es el modo de determinar cuándo una situación está sujeta a una privacidad normativa y cuándo no lo está. Esta cuestión es capital y problemática de resolver pues cada cultura determina lo que se entiende por normativamente privado. Incluso en el seno de cada cultura puede haber cambios en su interpretación. Como se ha visto en páginas anteriores la respuesta a este relativismo cultural es entender la privacidad como un valor fundamental. "I emphasize the core values because provide a common value framework, a set of standards, by which we can assess the activities of different people and different cultures*"* (Moor, 1997, p. 22). Existe así mismo, otra respuesta a esta cuestión determinada por argumentos, según él, de tipo racional y moral.

> In general, privacy allows one to gain goods such as enhancing liberty and controlling personal development and to avoid evils such as suffering psychological and economic losses. But, privacy is not an unalloyed good for it has its costs as well.
> (Moor, 1990, p. 77)

Siguiendo con el ejemplo de la información médica, el uso de este tipo de información para realizar estudios que permitan salvar vidas humanas o avanzar hacia la cura o el tratamiento eficaz de determinadas enfermedades puede significar para una sociedad concreta un bien general. En este caso puede que se esté disminuyendo la privacidad de uno o varios individuos pero se está realizando para el beneficio de la sociedad en general, lo que para Moor debe considerarse como un valor fundamental.

En lo que respecta a las tecnologías digitales, Moor sostiene que amplían, contrariamente a lo que podría creerse, los márgenes para la privacidad. Éstas permiten un espectro más amplio de situaciones normativamente privadas, en la medida en que permiten realizar acciones que antes estaban sujetas a la obligatoriedad de hacerlas en espacios públicos, como realizar la compra, hacer transacciones monetarias o ir a trabajar. "Without all of these modern technologies, our lives arguably would be much less private than they are now*"* (Moor, 1990, p. 79). La cuestión radica en saber dónde hay que poner restricciones en el uso de estas tecnologías para proteger la privacidad, ya que como afirma más adelante, "computer technology can protect zones of privacy as well as invade them*"* (Moor, 1990, p. 80).

4.5. Privacidad en público

Las tecnologías digitales han introducido en el debate ético sobre la privacidad un aspecto que hasta ahora no era tenido en cuenta como un tema a tratar o, al menos, no se había desarrollado de un modo lo suficientemente fructífero como para ser objeto de estudio en sí mismo. Autores como Herman Tavani o Helen Nissenbaum han tratado esta cuestión que puede entenderse o definirse como la privacidad en público.

En algún momento de esta investigación ya se ha dicho que parte de la información aparecida en el ciberespacio puede no haber sido generada por la persona o personas a las cuales se refiere dicha información. La capacidad de almacenamiento y la estructura basada en nodos del ciberespacio permite la difusión de información sin que se puede mantener un control real sobre la misma. Una vez que la información se ha digitalizado ésta se vuelve *grasienta* (Moor 1997, p 27), entendiendo por esto que es difícil mantenerla en un único espacio acotado y controlado. A medida que se mueve por el ciberespacio la información va dejando un rastro a su paso y se va incorporando a los nuevos lugares por los que circula, de modo que se crea una copia de esa información por donde ha circulado. Esta multiplicación de la información (de una misma información se entiende) es lo que le da el carácter grasiento del que habla Moor y aquello que dificulta el control sobre la misma. "We don't control vast amounts of information about ourselves. Personal information about us is well greased and slides rapidly through computer systems around the world, around the clock" (Moor, 1997, p. 31).

Es por eso que, "there could also be personal information on these Web pages that an individual has neither included nor explicitly authorized to have placed on a Web site" (Tavani, 2005, p. 40).

Supóngase que estando en la calle un ciudadano o ciudadana firma una petición para que se dejen de utilizar animales en la fiestas populares. En un primer momento esa información, esos datos personales como nombre, dni y firma, no tendrían porqué aparecer en ningún sitio web y no se esperaría que se difundieran más allá de la propia petición y la dirección a la que en un principio se fueran a remitir todas esas firmas colectivas.

Ahora bien, la organización o asociación que recoge las firmas podrá digitalizar toda la información recogida, pues tal vez quieran enviarla por correo electrónico o crear una base de datos de posibles futuros colaboradores con la causa. También puede suceder que quieran incluir en su página web esa información para fomentar y advertir al público en general que existe un determinado número de personas que está en contra del uso de animales en las fiestas populares. Esa información a su vez puede ser compartida con otras asociaciones o agrupaciones con intereses similares o tomada para realizar algún tipo de estudio. Todas estas acciones, posibilitadas por la digitalización de la información, implican que los datos de una persona, que firmó un papel en la calle, puedan aparecer y multiplicarse en la red sin que se haya dado un consentimiento explícito para ello.

La cuestión que se plantean autores como Tavani o Nissenbaum radica en saber si esa información contenida en el ciberespacio debe protegerse normativamente o si, por el contrario, no necesita de ninguna protección concreta al tratarse, en virtud de estar contenida en la red, como información pública.

Para intentar resolver esta cuestión, Tavani, por su parte, distingue entre dos tipos de información personal. Una información personal no pública que sería aquella relacionada con datos confidenciales como pueden ser los datos bancarios, o sensibles, como los informes médicos, entre otros. Un segundo tipo serían los relativos a información personal pública. En este caso estaría la información relacionada con el lugar de trabajo o estudios o la marca y el color de coche que conduce una persona, por poner unos ejemplos.

Hasta la incorporación de las tecnologías digitales como medio estandarizado de comunicación las cuestiones relativas al segundo tipo de información no presentaban ningún tipo de cuestión ética. “Imagine, for example, a scenario in which eigthy years ago a citizen petitioned his or her congressional representative to draft legislation that would protect the privay of each citizen’s movements in public places*”* (Tavani, 2005, p. 43).

Haciendo uso de la definición de Moor, aquella que tenía que ver con el concepto de situación (página 92 y ss.), Tavani aboga por considerar que si la información contenida en el ciberespacio pertenece a una situación normativamente privada, entonces se deben realizar los mecanismos necesarios para la protección de esa información. Por otra parte, cuando se trate de información que no se considera normativamente privada, que él considera como información personal pública, se deberá dejar que fluya libremente si se quiere que el ciberespacio siga funcionando como elemento comunicativo. Esto vendría a confirmar la propuesta de Moor de encontrar zonas o situaciones de privacidad donde el derecho a ésta y a la libertad estén respetados y protegidos por igual.

> Should practices involving the access of personal information on the Internet via search-engine technology be declared a normatively private situation? If we begin to think of personal information on the Web as constituting (Moor's notion of) a normatively private situation, we can also begin to think about some ways that this information can be protected in certain ways while other kinds of information – i.e., non-personal information – currently accessible to search engines can continue to flow easily.
> (Tavani, 2005, p. 44)

Por su parte, Helen Nissenbaum ha tratado el tema de la privacidad en público desde la perspectiva de la legalidad. Su preocupación se debe a que "in the public arena, people have become targets of surveillance at just about turn os their lives" (Nissenbaum, 1998 p. 3). Esta vigilancia, que se traduce en recolección de información de forma masiva, es para la autora la marca distintiva de la tecnología informática. No se trata de individualizar la información de modo que gobiernos o empresas conozcan los movimientos de cada individuo en el ciberespacio, su propuesta no parte de la idea de una vigilancia masiva con algún tipo de fin concreto al modo orweliano. Se trata más bien de una situación intrínseca a las tecnologías mismas. La capacidad de producir y almacenar información de las tecnologías digitales es precisamente lo que les lleva a producirla y almacenarla.

Esta flexibilidad, la posibilidad de almacenamiento y generación de información, la capacidad misma de gestión de los datos, es lo que determina la preocupación ante esta situación. No es una preocupación concreta a que los datos de los usuarios sean usados o a que éstos sean vigilados por los gobiernos y las instituciones sino ante la simple capacidad de hacerlo.

> [...] harvesting of information is held deeply under suspicion not only because it is seen as the significant driver of the unquenchable thirst for information about persons as well as its seemingly endless supply, but also because people perceive it to be illegitimate. (Nissenbaum, 1998, p. 4)

La recolección masiva de datos por un lado y la sensación de desprotección ante esta situación por otro, se debe a que existe una ausencia de un marco teórico robusto y coherente que permita una práctica ética en las tecnologías digitales. Las propuestas fragmentadas, inconexas y, a veces, contradictorias no permiten avanzar en el desarrollo de unas bases normativas en las cuales pueda apoyarse el ciberespacio y la ciberética. En el caso de la privacidad en público esta ausencia es más destacada que en otros ámbitos. Según Nissenbaum esto se debe a, principalmente, tres factores distintos pero interrelacionados.

El primero es un factor conceptual y que tiene que ver con la distinción dicotómica entre lo público y lo privado, mantenida en el ciberespacio por la tradición filosófica. Mientras lo público se ha tenido siempre como aquello relacionado con el gobierno y la comunidad, lo privado se ha reservado tradicionalmente a la familia, los ciudadanos singulares o las empresas (privadas). “In some contexts, for example, the term "private" indicates the realm of familial and other personal or intimate relations, while the term "public" indicates the civic realm or realm of community outside of this personal one” (Nissenbaum, 1998, p. 8).

Desde el punto de vista legal, lo público se ha tenido como relativo a los organismos y agencias oficiales mientras que lo privado se ha relegado al ámbito de cada individuo como ciudadano. En este contexto “the term "private" generally marks a distinctive area dedicated to settling scores between people in their capacities as private citizens, in contrast with "public" law, which generally covers disputes in which officials or agencies of government are involved” (Nissenbaum, 2000, p. 8). De esta distinción se ha dispuesto que el valor de la privacidad sólo debía atenderse en el ámbito de lo privado y que aquello público no debía tenerse como protegido en la medida en que es la propia sociedad o las instituciones quienes mediaban en las posibles circunstancias que pudieran darse.

En segundo lugar se da un factor normativo. La dicotomía entre lo público y privado lleva a los teóricos y estudiosos a tener que elegir, unas veces de forma explícita y otras de una forma no

intencionada entre uno de los dos aspectos, y poner de relieve la necesidad de proteger uno y no otro alegando que la protección de ambos puede llevar a un conflicto legal. Esto supone que al proteger la privacidad de un asunto se puede estar vulnerando el derecho o la libertad de otro. "Privacy in public is frequently a victim of such balancing as it regularly succumbs to the apparently overwhelming weight of competing interest*"* (Nissenbaum, 1998, p. 10).

Este argumento, que la autora llama *normative knock-down,* supone que en el espacio público y en virtud a su carácter abierto, no puede haber una expectativa de poner límites a la exposición que en él se esté haciendo. Una persona que realice una acción en un espacio público no puede esperar ningún tipo de privacidad ya que ésta estaría coartando la libertad de las personas que le pueden ver en ese espacio público realizar dicha acción. Este argumento suele ser esgrimido, en opinión de la autora, para argumentar que la privacidad en público no puede tenerse en consideración en la medida en que siempre entrará en conflicto con otros valores, como son la libertad de acción o de expresión.

El tercer factor tiene un carácter empírico. Esta cuestión, que bien podría extenderse a todos los aspectos relacionados con la ética del ciberespacio y no sólo atender a la privacidad en público, tiene que ver con los cambios que las tecnologías digitales han supuesto en todos los ámbitos de la vida. Unos cambios que la filosofía todavía no ha asimilado y que la retrasan a la hora de plantearse problemas y por lo tanto soluciones para los mismos[57].

> I sugest that the divergence of philosophical theory from popular resentment of surveillance practices is due, in significant measure, to critical changes which philosophical theory has not yet absorbed because, quite simply, prior to key development in information technology, the problem did not exist in a compelling form.
> (Nissenbaum, 1998, p 14)

Estos aspectos conceptuales, normativos y empíricos han llevado a las teorías filosóficas a dejar de lado la privacidad en público. La vigilancia de los ciudadanos y ciberciudadanos en los espacios públicos se ha relegado o mantenido en la esfera de los asuntos políticos y por ende a cuestiones

[57] La cuestión planteada al comienzo de esta investigación sobre si la ética está preparada para hacer frente a los cambios que traen consigo las tecnologías digitales parece surgir también aquí al cuestionarse la autora la capacidad actual de la filosofía de hacer frente a la cuestión de la privacidad pública.

que tienen que gestionarse en el ámbito también de lo público, esto es, entre los gobiernos y los ciudadanos.

Dos aspectos destaca la autora para alertar y reflexionar sobre esta situación. El primero y más destacado es la creciente incomodidad y preocupación en la que se encuentran los propios ciudadanos ante la vigilancia y recolección de datos personales por parte, ya no sólo de las empresas tecnológicas sino, de prácticamente todos los organismos sociales e institucionales, tanto públicos como privados, hecho que se ha analizado en esta investigación al hablar de los *Enenmigos de Internet* propuestos por RSF (páginas 59 y ss.).

Por otra parte y a modo de crítica, expresa su disconformidad ante los esfuerzos de algunos autores de esquivar la idea de someter la privacidad en público al derecho a la privacidad. El modo en que la privacidad en público se ve relacionada con el derecho a la privacidad tiene que ver con el movimiento de información de un contexto a otro, donde el sujeto pierde el control sobre esa información así como con las múltiples formas de manipulación de dicha información en tanto que puede recolectarse, clasificarse y recombinarse de diversas formas.

> I explore two key aspects public data harvesting. One is the practice of shifting information from one context to another (hecho que también se ha visto en el ejemplo de la recolección de firmas en la calle al hablar de Tavani)[...] A second is the set of practices involving collection, collation, and combination of information drawn from diverse sources in activities [...]I will argue that these two aspects of public surveillance make privacy an issue which adequate theories of privacy must cover, alongside the issues that have traditionally been acknowledged as part of their territory.
> (Nissenbaum, 2000, p. 19)

Para combatir ambas situaciones propone dos principios. El primero de ellos en una “honestidad contextual”. Esto significa la exigencia de la creación y aplicación de mecanismos que permitan limitar y mantener un cierto control sobre el traspaso de información de un lugar y/o formato a otro. Un segundo principio que estaría relacionado con la regulación sobre el posible uso de la información disponible.

> The idea of contextual integrity and the norms emerging from it ought not be utterly foreign. There is, after all ample precedent in relationships that explicitly call for confidentiality such as, physician to patient, clergyman to congregant, and so on. [...] This second approach accords a strong, comprehensive right to privacy which grants control to individuals over all information about themselves irrespective of context. (Nissenbaum, 2000, p. 31)

4.6. Privacidad como conocimiento de información personal no documentada

Como último ejemplo que se mostrará sobre las diferentes visiones de cómo puede entenderse la privacidad en el ciberespacio se expone la propuesta por William Parent. La definición de Parent es interesante para el estudio de la ciberética en general y en el ejemplo de Google en particular, ya que tal vez sea la que mejor explique el estado de cosas que suceden en la red y el modo en que la empresa ejemplo actúa.

Lo que distingue la definición de Parent de las que se han mostrado más arriba es que la de éste se basa en el contenido y no en el control de la información. Para Parent, "privacy is the condition of a person's not having undocumented personal information about himself known by others" (Parent, 1983, p. 346). Como Tavani, Parent distingue dos tipos de información personal. Por un lado se encuentra la información personal, que sería aquella relativa a una persona en concreto y que la distingue del resto. El nombre junto con el apellido estarían dentro de este tipo de información.

Por otra parte, existe otro tipo de información que si bien a la mayoría de la gente no le importa revelar, puede suceder que para determinadas personas sea información sensible. La altura, el peso, el número de pie, el lugar de residencia, el número de teléfono o el lugar de trabajo son considerados por Parent como hechos que pueden ser tenidos como sensibles para determinadas personas. Piénsese en una persona a la que le importa mucho su altura. Solo las personas cercanas a ella saben su altura en centímetros y el resto puede hacerse sólo una ligera idea ya que la persona en cuestión intenta ocultar, dentro de lo posible, su altura con el uso de tacones, alzas y evitando colocarse cerca de personas mucho más altas que ella. Para Parent, el hecho de desvelar la altura real de esa persona se debe considerar como una invasión de la privacidad.

> In light os these kinds of cases, let us adopt the following, more comprehensive definition: "personal information" refers either to facts that most persons in a given

> society choose not to reveal about themselves (except to friends, family, advisors, etc.) or to facts about which a particular person is extremely sensitive and which he therefore does not choose to reveal about himself (even though most other persons don't care whether these same facts about themselves are widely known).
> (Parent, 1983a, p. 346-347)

Mientras la información personal de las personas se mantenga oculta a la vista pública o se adscriba sólo a un núcleo pequeño e íntimo de personas seguirá siendo información privada. Ahora bien, una vez esa información se desvele como información pública, la persona o personas a las cuales se refiera esa información habrán perdido su capacidad de considerar tal información como privada, "for this reason special precautions are usually taken to ensure that the information does not became public property" (Parent, 1983b, p. 271).

El control sobre o acceso a la información son para Parent confusiones, debidas a la asimilación de la privacidad y la libertad como sinónimos. "I believe the voluntary disclosure counterexample is symptomatic of a deep confusion underlying the thesis that privacy is a form of control. It is a conceptual confusion, the mistaking of privacy for a part of liberty" (Parent, 1983, p. 273). En defensa de su noción de privacidad expone una serie de definiciones que considera necesario recordar y clarificar para distinguir la privacidad del resto de acepciones.

Define los conceptos de privacidad, libertad, autonomía, paz, salud, propiedad, soledad, seclusión, secretismo y anonimato, conceptos que han sido utilizados para definir la privacidad. Entiende que conceptualizar la privacidad como control sobre la información deja de lado, en su opinión, situaciones en las que las personas decidan voluntariamente divulgar su información personal. Su propuesta es que no se puede argumentar que esas personas en cuestión estén protegiendo o vulnerando su privacidad sino simplemente que están renunciando a ella. Los motivos por los que esto sucede pueden ser diversos y justificados. Una teoría de la privacidad debe tener en cuenta estas cuestiones y, en opinión del autor, la teoría del control sobre la información no las tiene.

Para justificar el motivo por el cual las personas, en sociedades occidentales, prefieren una definición como la que propone enumera una serie de razones. En primer estaría el poder que se ejerce sobre las personas cuando se dispone de información personal de las mismas. En su opinión,

la conexión entre daño e invasión de la privacidad explica los motivos por los que se respeta y/o se teme la información personal no documentada de las personas.

En segundo apunta a la intolerancia de las personas hacia formas de vida y de pensamiento diferentes a la propia. Esa "debilidad humana", como él la define, que se traduce en burlas y menosprecio de las creencias y costumbres ajenas llevaría a las personas a mantener la información personal en el terreno de lo privado e íntimo.

La tercera razón, basada en una "ética liberal" supone que hay cierta información que se desea mantener en privado. En la medida en que las personas deben tratarse como fines en sí mismos y no como meros medios para conseguir objetivos, se debe respetar ese espacio de intimidad que de otro modo podría dar como resultado, en virtud de la primera razón, una lucha de fuerzas desigual donde la información que se tenga de la(s) persona(s) sea utilizada en beneficio propio y menosprecio de otros.

Por estos motivos considera que la privacidad es un valor que hay que perseguir en la medida de lo posible. *"*Now I want to suggest that anyone who deliberately and without justification frustates or contravenes our desire for privacy violates the distinctively liberal, moral principle of respect for persons" (Parent, 1983b, p. 277). Ahora bien, por otro lado afirma que no pretende afirmar que el derecho moral a la privacidad suponga que ésta nunca debe ser invadida. Bien al contrario, su propuesta parte de la idea de enfatizar el derecho a no ser víctimas de una invasión de la privacidad injustificada.

La pregunta subsiguiente es la de saber distinguir cuándo una invasión de la privacidad se está realizando de un modo justificado o no. Para saber si la privacidad está siendo quebrantada injustamente, propone seis cuestiones fundamentales. Las primeras cuatro tienen que ver con la razón fundamental de la invasión de la privacidad. La quinta hace referencia a los mecanismos que se han realizado para que no suceda y la sexta a las herramientas para la no trascendencia de la invasión una vez que suceda.

1. For what purpose(s) is the undocumented personal knowledge sought?
2. Is this purpose a legitimate and important one?

3. Is the knowledge sought through invasion of privacy relevant to its justifying purpose?
4. Is invasion of privacy the only or the least offensive means of obtaining the knowledge?
5. What restrictions or procedural restraints have been placed on the privacy-invading techniques?
6. What protection is to be afforded the personal knowledge once it has been acquired?

(Parent, 1983b, p. 281)

Estas preguntas deberían ser suficientes para responder a los casos particulares partiendo de la definición dada de privacidad. En el caso de Google, como se verá en su momento, estas preguntas tienen unas respuestas técnicas y económicas que podrían resultar insuficientes para justificar una pérdida de la privacidad o una invasión injustificada de la misma. Por otro lado, en la medida en que toda la información contenida en la red puede entenderse como información documentada resultará complicado, según los argumentos de Parent, clasificarla como información personal.

4.7. El utilitarismo y la cuestión de la privacidad en el ciberespacio

Al comienzo de esta investigación (página 13) se ha explicado brevemente la teoría ética utilitarista. Dentro de esta corriente se pueden distinguir dos tipos básicos de esta teoría. Por un lado estaría el utilitarismo de la regla, que afirma que una acción es correcta, esto es moralmente buena, si se rige por una norma que aporte mayor utilidad a un mayor número de personas. Mientras que el utilitarismo del acto es aquel que mide la bondad de una acción en función de la cantidad de bienestar que produzca esa acción. Una persona puede pensar que mentir es moralmente reprobable en cualquier circunstancia estando así manteniendo un argumento utilitarista de la norma. Mientras que otra puede opinar que mentir es algo reprobable en función de los motivos y las consecuencias de esa falsedad, sosteniendo su argumento en un utilitarismo del acto.

Analizar la privacidad en términos utilitaristas puede ser un camino complicado, en la medida en que determinadas posturas tiendan a apoyar un utilitarismo de la regla y en otras circunstancias dirigirse a una del acto. La pedofilia, por ejemplo, no siendo un ejemplo exclusivo de las tecnologías digitales, supone una cuestión de preocupación fundamental en el ciberespacio, debido

a las posibilidades que éste permite para la difusión de este tipo de material digital y es un buen ejemplo donde se puede observar esa dualidad de posiciones utilitaristas.

Póngase por caso a una persona que genera, almacena y distribuye pornografía infantil por Internet. Nadie niega que es un acto reprobable y censurable y que sería una acción correcta, ergo moral, atrapar a la persona en cuestión. Acabar y destruir con toda la información relativa a este hecho de sus dispositivos, sus cuentas personales, sus redes sociales relacionadas y todo el contenido pedófilo en general del que disponga. Para conseguir ese tipo de información, esto es, demostrar que esa persona efectivamente posee ese contenido, se tienen que realizar una serie de pasos.

En primer lugar se tiene que rastrear la red en busca de ese tipo de contenido concreto. Se rastrean multitud de páginas web, de foros, de perfiles de redes sociales, etc. Una vez que se detectan indicios que permitan inferir que puede existir contenido sexual infantil, se continúa siguiendo la huella digital de la persona en cuestión que se crea lo produce. Monitorizando sus pasos por la red se ha de confirmar que efectivamente esa persona tiene en su disposición información de esa índole. Puede que sea consumidora de pornografía infantil pero que no sea ella misma quién la almacene, produzca y distribuya. La acción sería reprochable y condenable de todos modos pero no en la misma medida que aquella persona que genere el contenido, del mismo modo que un consumidor de droga no puede ser condenado en la misma medida que un traficante o un proxeneta igual que un usuario de los servicios de acompañantes. La comprobación de ese contenido pasa entonces por la vigilancia de la persona (y las personas usuarias). Una vigilancia que puede incluir el acceso a sus cuentas de correo, sus dispositivos electrónicos, memorias externas y en algunos casos el registro de la vivienda o locales.

La pregunta que surge es si esa(s) persona(s) tiene(n) derecho a la privacidad en el ciberespacio. Hay que tener en cuenta que para llegar a localizar información relativa a la pornografía infantil se ha de tener acceso a cualquier contenido que contengan sus dispositivos para poder determinar qué datos son pornográficos y cuales no. Sus dispositivos pueden contener datos sobre la familia, el trabajo, sus relaciones sociales o su historial médico. Por otra parte, para descartar que otras personas de su entorno compartan con ella ese interés habrá que vigilar y monitorizar sus contactos en el ciberespacio.

De acuerdo con la postura utilitarista que se sostenga la respuesta a esta cuestión será diversa. Si la posición que se adopta es la de un utilitarismo del acto, la pérdida de privacidad de la persona investigada maximiza el bienestar general, en la medida en que se acaba con una acción injusta e ilegal en la sociedad actual. Es cierto que otras personas pueden verse afectadas por esa vigilancia y que en esos casos, de forma individual, se está realizando una acción injusta. Pero existe una justificación superior que es la de atrapar a una persona pedófila y proteger los derechos de las personas menores. En este caso, la protección y privacidad de los y las menores es más importante en términos morales que salvaguardar la privacidad de los adultos pedófilos. En este caso, la vigilancia de las telecomunicaciones que lleve a atrapar a un pedófilo está justificada moralmente.

Si se atiende al utilitarismo de la regla la cuestión es más complicada. Si la norma que se ha de seguir es la de respetar la privacidad de las personas, sean cuales sean las circunstancias, entonces no está justificada la vigilancia de una persona, independientemente de cuales sean sus actos. Se puede argumentar que lo que se defiende en este caso es la privacidad de los niños y niñas que están siendo objeto de abuso y que esta defensa está por encima de la privacidad de las personas adultas. Así la privacidad de un persona es defendible normativamente siempre y cuando no entre en conflicto con la privacidad de otra persona, en este caso, personas infantiles. Ahora bien, si la privacidad es un valor que hay que proteger per se, como afirmaría el utilitarismo de la regla, y ésta, en este ejemplo en cuestión, solo puede ser protegida violando el derecho de privacidad de otra persona, esta postura resulta paradójica.

Esta situación ya se ha presentado en los argumentos de Anita Allen a la hora de abordar el tema de la privacidad en términos de acceso a la información. Por un lado se debe proteger la privacidad de las personas pero por otra parte hay que tener cuidado que esa protección no lleve a la desprotección ante determinadas circunstancias. En su ejemplo había que proteger el acceso a la vida personal de las mujeres para que éstas puedan tener una autonomía en cuanto a su vida reproductiva se refiere al tiempo que hay que vigilar que ese control sobre el acceso a su privacidad no desemboca en situaciones de desamparo a la hora de abordar cuestiones como el maltrato en la vida privada.

A la luz de estas situaciones, en las que el utilitarismo de la regla se encuentra con dificultades a la hora de tratar el tema de la privacidad en el ciberespacio, lo que en términos de Moor sería no atender a las *situaciones,* parece no ser una teoría apropiada para mantener la red como un espacio

de comunicación compartida y defender, al mismo tiempo, la privacidad de cada uno de los ciberciudadanos.

Por otra parte, tampoco parece que el utilitarismo del acto resuelva el problema de la privacidad. Pues en la medida en que se introduce la posibilidad de desprotegerla, con independencia de los motivos que se esgriman en cada caso, se pueden encontrar para cada circunstancia y cada sujeto motivos, siempre suficientes, para vulnerar la privacidad de alguien.

Sin embargo, a pesar de estas dificultades, los autores y autoras que se han analizado anteriormente parecen sostener un utilitarismo de la regla a la hora de exponer sus argumentos. Con independencia de apoyar explícitamente o no la privacidad como un valor intrínseco, lo cierto es que sus posturas tienden a defenderla como si de facto la tuvieran como un valor esencial que se ha de salvaguardar y por lo tanto se sitúan en una postura donde la regla moral en el ciberespacio es proteger la privacidad de las personas en cualquier caso.

En el momento en que se han de apoyar en un utilitarismo del acto, como en el caso ya mencionado de Anita Allen, cuando se trata de cruce de datos entre médicos, a la hora de vulnerar la privacidad de algunas personas por salvaguardar la privacidad de otras o cuando se diferencia o no entre el espacio público y el privado, en todos estos caso lo cierto es que se está manteniendo una visión de la privacidad como un valor fundamental que debe conservarse salvo en los casos en los que sea estrictamente necesario no hacerlo.

Parece que el concepto de privacidad que mantienen les lleve a pivotar entre un utilitarismo de la regla y uno del acto en función de las circunstancias. Esta situación podría llevar a pensar que en realidad mantienen que en determinadas circunstancias se ha de actuar conforme a las consecuencias de los actos y que, por lo tanto, lo que defienden es un utilitarismo del acto. Pero, al mismo tiempo, es la defensa de la privacidad, como norma, lo que les lleva a actuar de tal modo, situándose de este modo en un utilitarismo de la regla.

Esta postura ante la privacidad en el ciberespacio, una postura que tiende a conservarla y a tenerla como un derecho que deber ser protegido de las injerencias externas conlleva muchos problemas a la hora de encontrar un consenso sobre cómo ha de ser tratada y aleja el debate teórico de la realidad y la práctica del ciberespacio. La idoneidad de este enfoque se analizará más adelante

cuando se haya visto cómo trata Google la privacidad de sus usuarios en sus servicios. Tan solo adelantar en este momento dos cuestiones. La primera de ellas es la adecuación, en cualquier caso, de la postura utilitarista como ética para hablar del ciberespacio. El problema no radica en la teoría en sí sino en el contenido que con ella se analiza. Este contenido, y aquí la segunda cuestión, es el de una concepción de la privacidad que se adelanta aquí como una "privacidad analógica".

4.8. Resumen

Como se ha visto en las páginas precedentes no existe un consenso sobre qué se ha de entender por privacidad. Aunque existen más autores y autoras que han tratado el tema que los aquí expuestos éstos suponen los representantes más destacados de las teorías que se pueden encontrar al respecto. Se ha dicho que no hay un acuerdo sobre una definición para el concepto de privacidad pero a pesar de ello se pueden encontrar puntos en común entre todas las teorías analizadas.

En primer lugar se puede afirmar que, como se ha hecho explícito al comienzo de este capítulo, existe un acuerdo sobre la importancia de la información a la hora de tratar el tema de privacidad. También se ha mostrado como ésta es uno de los temas más tempranos en el debate ético en las tecnologías digitales. La capacidad de producción, almacenamiento, movimiento y recombinación de la información que han supuesto estas tecnologías ha llevado a los profesionales y académicos, así como al público en general, a preocuparse por los motivos, las razones y las formas en que se utiliza esa información.

Dentro de ese debate se ha tratado la distinción entre el aspecto público y privado de la información. Todos los autores presentados, de un modo u otro, expresan sus teorías haciendo explícitos ambos conceptos ya sea para situar el derecho a la privacidad en el espacio privado o para extenderla al público. Una distinción que, como se ha visto, se remonta a Aristóteles y que hoy en día genera debate en torno a los límites de la privacidad y el derecho a la misma. La monitorización del espacio público por un lado y la inclusión de las actividades tradicionalmente publicas en el ámbito privado ha llevado a que las fronteras entre ambos espacios se vean difuminadas y que sea necesario hablar de una privacidad de lo público y de una recontextualización de lo privado.

En tercer lugar todos ellos comparten la idea de que la privacidad es algo que hay que proteger y defender, esto es, que tiene un valor. Ya sea un valor para alcanzar cierto estado de cosas, como las relaciones personales, la fraternidad o la autonomía o bien como un valor en sí mismo. El valor de

la seguridad, como afirmara Moor, presente en todas las sociedades, supondría un reflejo de la privacidad.

Estas son las convergencias entre todos los autores: privacidad informativa, reinos de lo público y privado y valor. A partir de aquí cada autor se dirige por caminos diferentes a la hora de interpretar la privacidad, y lo que para unos es control para otros es acceso a la información. Se han revisado varios autores que tratan la privacidad como control sobre la información. Según esta perspectiva, la privacidad partiría del control de cada individuo respecto a la información que quiere dar. Entre estos autores se encuentran Fried y Westin, para quienes lo fundamental es tener control sobre cuánta, a quién, en qué momento y para qué se comparte información personal con otras personas.

Por otra parte se ha visto que otros autores, entre las que estarían Gavison y Allen, proponen una privacidad basada en el acceso a la información. Así pues, lo importante no sería mantener el control sobre la información sino sobre quién tiene acceso a la misma. Se ha visto como existen ocasiones en las que el control de la información es inexistente y que lo importante es quién tiene acceso a ella. Gavison aportaba la idea de una privacidad perfecta basada en la soledad. Allen, por su parte, ponía el acento en la dificultad del acceso de la información a la hora de proteger la vida pública y privada de las personas.

James Moor proponía una combinación de ambas teorías basando la suya en el concepto de situación. Su propuesta, una privacidad como acceso restringido y controlado de la información supone la demarcación de situaciones, de zonas privadas basadas en la privacidad natural y normativa para soslayar los problemas derivados de las dos teorías anteriores.

Tavani y Nissenbaum abrían el debate en torno a la privacidad en público. Por su parte Tavani hablaba de dos tipos de información personal, una pública y otra privada. En esta distinción es donde, según él, hay que fijarse a la hora de tratar marcar los límites de la privacidad. Nissenabaum hacía hincapié en el problema de la monitorización y recolección masiva de datos sin un control determinado. Hecho que le lleva a plantearse la necesidad de unos nuevos límites para la privacidad que tienen que ver ahora también con el espacio público.

Por último se ha tratado la propuesta de Parent de una privacidad basada en el conocimiento de información personal no documentada. Para este autor, la privacidad tenía que ver con el contenido

de la información y no sobre el control de la misma. Aquello que debe ser tenido como privado son los datos personales de una persona que no han sido documentados por ningún medio, esto es, información que sólo la persona y los allegados con los que ella haya querido compartir esa información personal posean. Toda información que no se mantenga en este ámbito de lo no documentado pasa a pertenecer al ámbito de lo público donde el poseedor inicial pierde su derecho a la privacidad. Ahora bien, también se veía la posibilidad de que exista una violación del derecho a la privacidad que tenían que ver con los motivos y los medios por los que esa información había sido desvelada y proponía una serie de cuestiones para confirmar o no la injusticia de una invasión de la privacidad.

CAPÍTULO 5:
LA PRIVACIDAD EN GOOGLE

Las empresas tecnológicas y las proveedoras de servicios en Internet son conscientes de la preocupación ante el uso que pueda hacerse de la información proporcionada por sus usuarios. Lejos de ignorarla o subestimarla se afanan por hacer ver al usuario que esta preocupación es compartida. Así, muchas de ellas, en sus apartados de "políticas de privacidad" comienzan afirmando que la privacidad de los usuarios es algo importante para la empresa. Esto puede verse en Microsoft[58], Apple[59] o Google[60]. Como se ha mostrado en el capítulo anterior la privacidad ocupa también un lugar predominante en los intereses de la ciberética. De este modo, teóricos, empresas y usuarios comparten la idea de que la privacidad es algo importante en las tecnologías digitales.

Mientras que la ciberética se preocupa por entender qué es la privacidad en el ciberespacio, qué datos deben ser tratados como confidenciales, en qué medida se debe almacenar y procesar la información, cuándo están justificadas estas actuaciones y cómo se puede impedir o minimizar el daño que pueda causar ese tratamiento informativo, las empresas tecnológicas vuelcan sus esfuerzos en justificar la necesidad de tratar la privacidad de modo que se mantenga el funcionamiento y la conservación del ciberespacio.

Un motivo recurrente que esgrimen las empresas para recopilar, almacenar y gestionar información de sus usuarios es la denominada *experiencia de usuario.* Por ésta se entiende "the experience that a person gets when he/she interacts with a product in particular conditions" (L. Arhippainen, M. Tähti, 2003 p. 27). Una definición más precisa se encuentra en Knapp Bjerén que afirma ser "el conjunto de ideas, sensaciones y valoraciones del usuario resultado de la interacción con un producto; es resultado de los objetivos del usuario, las variables culturales y el diseño del interfaz*"* (Bjerén, 2003, p. 25).

5.1. Personalización y experiencia del usuario

El ciberespacio, y en concreto Internet, es un lugar excesivamente grande como para que un usuario se encuentre cómodo navegando por la red sin señales o hitos que le marquen el camino. Podría hacerse el paralelismo con un barco y su capitán que intente navegar la mar sin instrumentos de navegación, sin la guía estelar para orientarse, sin referencias costeras que le sitúen en un lugar determinado y sin tripulación que lo acompañe. Ciertamente éste se encontraría perdido en una

[58] https://privacy.microsoft.com/es-es/privacystatement/

[59] https://www.apple.com/es/privacy/

[60] https://www.google.es/intl/es/policies/privacy/

situación así y sería difícil que llegara a su lugar de destino sin ninguna de estas herramientas que le permitan orientarse. Al cibernauta le sucedería algo similar sin marcas que le ayuden a navegar por el ciberespacio, de ahí la importancia de la experiencia del usuario y de la personalización de contenidos.

El diseño basado en la experiencia del usuario tiene como objetivo facilitar el uso de la tecnología y los interfaces, hacer de la usabilidad algo intuitivo y atractivo de modo que sea fácil y cómodo alcanzar los objetivos que tiene el usuario. Los índices de las páginas, los links de un lugar a otro o el lugar que ocupa cada elemento dentro de la web, son elementos que forman parte de la experiencia del usuario. Esta inquietud por hacer de Internet un lugar donde cada usuario encuentre rápidamente aquella información que le pueda resultar relevante, esto es, basada en sus intereses y afinidades ha llevado a los motores de búsqueda, las redes sociales, los medios de comunicación digitales o las empresas de publicidad en línea ha desarrollar una técnica denominada personalización de contenidos.

La personalización de contenidos, al menos en sus bases, tiene como objetivo contrarrestar lo que Alvin Toffler (1970) denominó como *information overload.* Su idea principal supone que al estar expuestos a demasiada información los individuos son incapaces de absorberla, procesarla y generar conocimiento. La sobrecarga informativa impide discernir entre información relevante y la que no lo es, dificultando la toma de decisiones a la hora de tomar una postura razonada sobre una cuestión concreta. Si bien es cierto que su visión, en el momento en que fue escrita, era considera como futurista y por lo tanto, especulativa, lo cierto es que algunas de sus preocupaciones son realidades hoy en día.

En primer lugar observó la "tensión y desorientación que provocamos en los individuos al obligarles a un cambio excesivo en un lapso de tiempo demasiado breve*"* (Toffler, 1970, p 2). Tensión y desorientación que se puede observar en las personas de la tercera edad interactuando con las tecnologías e incluso con personas inmigrantes digitales ante estas invenciones tecnológicas. Por otra parte expresaba la falta de habilidades humanas y cognoscitivas para afrontar ese cambio, un cambio que es más veloz que lo que el ser humano es capaz de procesar. "Me espantó, gradualmente, lo poco que saben hoy en día de adaptabilidad tanto los que exigen y producen grandes cambios en nuestra sociedad, como aquellos que pretenden prepararnos para hacer frente a tales cambios" (Toffler, 1970, p 2). Esta idea está presenta en la crítica aquí expuesta sobre la

resistencia a la hora de tratar el tema de la privacidad en el ciberespacio para asumir un cambio en el concepto mismo que estudian.

Esta sobrecarga informativa, que puede encontrarse también denominada como infoxificación o infobesidad, se ha resuelto, con mayor o menor acierto, a través de la personalización de contenidos. La personalización de contenidos pretende que los usuarios accedan a un contenido que sea relevante para sus intereses, gustos y afinidades. Para mostrar información relevante a cada usuario es necesario en primer lugar crear un modelo de usuario. Saber en qué lugar vive, su situación familiar, a qué se dedica, cómo invierte su tiempo libre, qué tipo de ropa viste, cuáles son sus amistades y las diferentes relaciones que tiene con éstas, si tiene mascota, si practica algún deporte, si es miembro de alguna asociación, club o comunidad, los viajes que realiza, etc. Toda información relacionada con el modo de vida del usuario es relevante y útil a la hora de personalizar los contenidos que se le ofrecen.

Una vez creado el modelo de usuario es necesaria una selección de contenidos acorde a ese modelo. Sería una pérdida de recursos y una personalización defectuosa el incluir publicidad sobre pruebas de embarazo en los resultados de búsqueda de un usuario que sea un hombre de ochenta años, del mismo modo que lo sería incluir en los de un adolescente anuncios sobre seguros de coche. De ahí que la selección de contenidos según el modelo de usuario es esencial, no sólo para la experiencia del usuario mismo sino también, para la optimización de los recursos de las empresas.

Una vez seleccionado el contenido que pueda ser interesante para el usuario se le presenta en forma de información. Hay que tener en cuenta que la personalización no se da en exclusiva en el ámbito de la publicidad, aunque sea en ésta donde encuentra su mayor exponente. Cuando se lee un periódico digital, por ejemplo, el simple hecho que se esté leyendo en una zona geográfica concreta determina la presentación y orden de la aparición de las noticias. Así mismo, según los vídeos que se hayan podido ver con anterioridad en plataformas como Youtube determinan las *sugerencias* que esa plataforma hace al usuario sobre posibles vídeos que le pueda interesar ver. En redes sociales como Facebook, cuanto más *cerca* como usuario se esté de un contacto, esto es, cuanto más afinidad tengan las personas conectadas en esta red social con un mismo modelo de usuario, más apariciones tendrán esas personas en sus muros. Cualquiera que tenga activo un perfil en esta red social es consciente de que cuanto más *me gusta* y más se interacciona con una persona, más tiempo

se mantiene esa persona entre las apariciones del muro. A medida que se deja de tener contacto virtual con esa persona, menos posibilidades hay de que aparezca en el muro del usuario.

En el motor de búsqueda Google se dan varios aspectos de personalización de contenidos. El primero y más evidente es el idioma. El buscador deduce que si se está realizando una búsqueda desde www.Google.es los resultados esperados por el usuario deben ser en castellano, si se realiza desde www.Google.fr serán en francés, desde www.Google.hk en chino, etc. Aunque también es cierto que estando en España, por ejemplo, aunque se realice una búsqueda desde www.Google.ru los resultados aparecerán en castellano y no en ruso. Esto se debe a que la IP desde la que se realiza la búsqueda está sita en España, por lo que se calcula que lo que espera el usuario son resultados en castellano. La personalización no deja de predecir que aunque se esté buscando desde el buscador de otro país el usuario está alojado en un país concreto y será el idioma de ese país el que utilice Google para mostrar los resultados, a no ser que el usuario especifique lo contrario. Es precisamente a través de la personalización (y del modelo de usuario) que Google puede predecir el idioma *preferido* por el usuario.

Otra herramienta de Google para mejorar la experiencia del usuario es la denomina da Google Instant o escritura predictiva. Para realizar una búsqueda cualquiera es necesario introducir una palabra o frase relacionada con la aquélla. Cuando se escriba la primera letra de la búsqueda, Google Instant mostrará varias opciones de resultados que comiencen con la letra escrita. Éstas tendrán que ver con las preferencias de búsqueda del usuario y con las tendencias de búsquedas en el momento de introducir la letra.

El SafeSearch o control parental es otra herramienta de Google que sirve para personalizar los contenidos. Ésta permite controlar los resultados que aparecerán (o no) al realizar una búsqueda. Se utiliza para omitir de los resultados, y por tanto restringir las búsquedas, determinado tipo de contenido, ya sea violento, explícitamente sexual o inadecuado para determinado grupo de población. Esta opción, igual que Google Instant se activa y desactiva desde el panel de configuración del buscador. Teniendo activado el SafeSearch búsquedas como “porno” no obtendrán ningún resultado, y haciendo una búsqueda de “vídeos porno” el buscador omitirá la palabra porno y mostrará sólo resultados relacionados con vídeos en general. El ejemplo de SafeSearch es una muestra de cómo la personalización de contenido permite la aparición o la omisión de determinada información disponible en la red.

Estos son algunos ejemplos de personalización de contenido que el usuario puede elegir en su buscador y por lo tanto le permiten tener cierto control sobre la personalización y la experiencia del usuario. Pero existen muchas otras herramientas y acciones, más o menos incontrolables por parte del usuario, que hacen que el motor de búsqueda clasifique, escoja y muestre al usuario determinados resultados sin que éste tenga forma activa de actuar sobre ellos.

En primer lugar están los propios resultados de búsqueda, denominados resultados orgánicos. Los resultados orgánicos son aquellos que son ofrecidos y mostrados en un orden concreto según la relevancia, medida por algoritmos, de una página o páginas y en función de la adecuación de esa página a la búsqueda realizada. Si se realiza una búsqueda desde España de "Coca Cola", por ejemplo, los algoritmos de Google calculan que debe aparecer, en primer lugar, la página oficial de la marca de bebidas y, en segundo lugar, que debido a la situación geográfica, la página oficial que debe aparecer es la española, así que mostrará como primer resultado www.cocacola.es. En función de la relevancia la segunda entrada (modo en que se denomina a los resultados) será la web Wikipedia y su artículo sobre la bebida, en tercer lugar aparecerá la cuenta de Twitter o Facebook de la compañía, en cuarto lugar la fundación benéfica de la empresa, etc.

En cambio si la búsqueda incluye la palabra "mata" y se realiza una búsqueda que sea "Coca Cola mata" entonces no aparecerá en los resultados ninguna de las web que estén relacionadas con la empresa, sino artículos, vídeos, blogs y otro tipo de información relativa a los inconvenientes y posibles problemas derivados del consumo de esta bebida. Los algoritmos de Google calculan en este caso diversas variables. En primer lugar que la empresa del refresco no tiene ninguna relevancia a la hora de tratar los efectos nocivos del consumo de la bebida y por lo tanto no debe aparecer en los resultados. En segundo lugar, que la persona que está realizando la búsqueda "Coca Cola mata" no tendrá interés en conocer la página web oficial de la compañía sino la información que pueda existir sobre lo negativo de la ingesta del refresco.

Los resultados orgánicos se ordenan y muestran al usuario en función de varios aspectos. En primer lugar está la relevancia mencionada anteriormente y que es calculada por el PageRank (páginas 19 y 20). En segundo lugar está el modelo de usuario. Si un usuario es un apasionado de los coches y utiliza Internet para la búsqueda de noticias sobre las nuevas tendencias automovilísticas o los próximos eventos relacionados con el tema y las noticias de los medios de comunicación sobre coches, al introducir la búsqueda "vendo vaca" lo más probable es que los primeros resultados

orgánicos ofrecidos por Google sean sobre empresas que venden vacas para coches, tiendas de segunda mano o páginas web donde particulares vendan y compren accesorios para coches, foros o revistas donde haya un tablón de anuncios con venta de este accesorio para los vehículos, etc. En cambio, si un empresario ganadero hace la misma búsqueda e introduce "vendo vaca" y utiliza Internet también para conocer las mejoras en el pienso para animales, los nuevos antibióticos, los impuestos sobre la venta de vacuno o la tendencia en el consumo de carne, entonces el resultado orgánico que se le ofrecerá a este usuario en concreto no será el de la venta de vacas para coches sino resultados que tengan que ver con las búsquedas que haya hecho con anterioridad y por lo tanto relacionados con la venta del animal vaca.

Estos resultados objetivados (objetivados porque se dirigen a un objetivo o usuario concreto) que en principio son resultados no manipulados, tienen la característica de estar personalizados. Se dice que no son manipulados porque se basan en la relevancia de cada web para cada búsqueda concreta y en principio dependen de un algoritmo y no de la injerencia humana. Pero la personalización implica que a cada usuario se le presente aquello que puede ser más relevante para sus intereses y modo de vida. De ahí que puedan existir diferencias en los resultados orgánicos entre usuarios. Este ajuste de los resultados para cada uno de los cibernautas hace que la experiencia del usuario sea más satisfactoria ya que cada persona encuentra en la red aquello que, en principio, se adecua más a sus gustos y a lo que posiblemente esté interesado en buscar.

Algo similar ocurre con los enlaces patrocinados. Un enlace patrocinado es un anuncio que se publica en la página de resultados de un buscador cuando un usuario realiza una búsqueda. Aparece en relación con esa búsqueda y una de sus características principales es que tiene la apariencia de un resultado orgánico. Esto tiene un gran valor para los anunciantes en la medida en que se aseguran que sus anuncios están llegando a un público que en principio está interesado en el producto. Por otra parte, los usuarios tienden a realizar clic sobre él, ya sea porque se confunde con un resultado orgánico, bien porque es un tipo de publicidad no invasiva (no hay diseño creativo) y siempre relacionada con la búsqueda realizada o bien porque se confía en que los primeros resultados que se ofrecen serán siempre los mejores. Así, si el usuario ha introducido una búsqueda sobre "cañas de pescar" los enlaces patrocinados serán anuncios donde se vendan cañas de pescar, aparejos de pesca, etc. Este tipo de publicidad, por su propia naturaleza relacionada con la búsqueda concreta del usuario es considerada como personalizada. Ayuda a la experiencia del usuario por su formato

adaptado al estilo del buscador y por su adecuación a las necesidades del usuario al tiempo que optimiza los recursos de los anunciantes.

5.1.1. La burbuja filtro

La personalización es una buena herramienta para navegar de un modo cómodo y adecuado a la experiencia particular de cada usuario. Permite encontrar rápidamente lo que se está buscando evitando navegar de una web a otra de un modo que podría decirse a ciegas. Así mismo, para las empresas que ofrecen sus productos y servicios en la red es una opción eficaz para llegar a un público objetivo sin tener que gastar recursos, también a ciegas, para llegar a él. Sin embargo, la personalización tiene sus contrapartidas y desventajas cuando se trata de encontrar puntos de vista diferentes al propio, ampliar los límites del usuario o simplemente descubrir cosas nuevas en la red.

Esta situación la ha definido Eli Pariser (2011) bajo el concepto de "burbuja filtro". Su idea principal es que, actualmente, la personalización lleva al usuario a permanecer en una burbuja informativa en la que es difícil introducir o dar con información que no se calcule relevante para el usuario. La personalización de contenidos lleva a que la información que aparece al usuario sea aquella que se ajusta al modelo de usuario que se ha formado del individuo, alejándole de información nueva, contraria a sus creencias y gustos o con puntos de vista diferentes al suyo propio. Esto lleva a que Internet, o más concretamente el buscador, muestre (ofrezca resultados de) aquello que considera (calcula) se quiere ver (cuadre más con el modelo de usuario), encerrando al individuo en una visión homogénea y constante. "First, the filter bubble surrounds us with ideas with which we're already familiar, making us overconfident in our mental framework. Second, it removes from our environment some of the key prompts that make us want to learn" (Pariser, 2011, p. 56).

A través de la personalización de contenidos, sostiene Pariser, las personas son alejadas de las que son diferentes a ellas, del mismo modo que las aleja de ideas, opiniones e información que no se corresponda con el modelo que se ha tomado de ellas. El problema surge cuando se confía a los algoritmos y al cálculo matemático la tarea de editar la información que se le presentará al usuario. Ambos métodos no tienen en cuenta la importancia cognitiva del error y la divergencia, así como tampoco un cuentan con un carácter ético, aquel que imprimían los seres humanos al realizar esas tareas de edición:

> Human beings may be a walking bundle of miscalculations, contradictions, and irrationalities, but we're built that way for a reason: The same cognitive processes that lead us down the road to error and tragedy are the root of our intelligence and our ability to cope with and survive in a changing world. We pay attention to our mental processes when the fail, but that distracts us from the fact that most of the time, our brains do amazingly well.
> (Pariser, 2011, p. 56)

Pónganse un ejemplo de lo que el autor considera como una burbuja filtro. Cuando una persona se interesa por un acontecimiento, como podría ser el intento de golpe de estado en Turquía en julio de 2016, buscará información en la red que pueda ampliar los conocimientos de la situación real. Los resultados de búsqueda sobre esa noticia vendrán determinados por las búsquedas anteriores. Si esa persona acostumbra a leer periódicos de carácter liberal, las noticias que aparecerán en las primeras posiciones serán de prensa o canales de televisión que tengan esa orientación política. Si por el contrario sus tendencias le orientan hacia un conservadurismo entonces los resultados que se le ofrezcan serán ofrecidos por canales o prensa de esa orientación. Sucederá lo mismo, afirma Pariser, con las redes sociales. Las opiniones sobre el intento del golpe de estado en Turquía del grupo de amigos que más cercanas estén a las opiniones de la persona serán las que aparezcan en su muro, mientras que se omitirán las que se alejan de su ideología. Así la persona sólo tendrá acceso a información ya conocida. La burbuja filtro alejará ideas nuevas o contrarias a las propias y limitará la ampliación de puntos de vista.

Otro ejemplo de cómo funciona la burbuja filtro se encuentra en las propias herramientas de personalización de Google. Es posible que un usuario sea aficionado a leer periódicos deportivos digitales y tenga activo el Google Instant pero que en un momento determinado esté interesado en leer alguna noticia sobre el intento de golpe de estado. Al introducir la letra "a" en su buscador lo más probable es que le aparezca como primer resultado la opción del periódico digital "*as"* y como segunda sugerencia *abc*. El usuario puede estar muy interesado en la noticia de la que quiere informarse y clique sobre la segunda opción, pero la personalización de contenidos le estará "recordando" que lo que le interesa es la prensa deportiva y llevando, de un modo muy sutil a olvidarse de su primer (y nuevo) interés y volver a abrir la web de la prensa deportiva.

Sin darse cuenta, la persona estará siendo dirigida a un modelo de sí misma, un modelo que no es elegido por el usuario, para cada situación y en cada momento, que le insta a permanecer en lo que en algún momento un cálculo matemático dedujo que era. Una acomodación a un modelo que le empuja a repetirse y mantenerse de modo que pueda ser predecible. Como afirmaba Eric Schmidt (director ejecutivo de Google desde 2001 hasta 2011 y actualmente presidente de Alphabet Inc.) en una entrevista realizada por Holman W. Jenkins Jr. para el Wall Street Journal en 2010, "The power of individual targeting—the technology will be so good it will be very hard for people to watch or consume something that has not in some sense been tailored for them"[61].

5.1.2. Personalización, experiencia del usuario y privacidad

Se ha visto cómo la personalización ayuda a mejorar la experiencia del usuario y cómo ésta es una parte del diseño del ciberespacio que permite a los cibernautas navegar en la red de un modo que no resulte ajeno y hostil. Pero como afirma Pariser, también puede volverse un problema cuando, de toda la información disponible en la red, los algoritmos muestran una pequeña parte escogida para el modelo de usuario que se ha creado a partir de intereses pasados.

Ahora bien, hay que tener en cuenta que tanto la personalización y la experiencia del usuario son herramientas que permiten a las personas navegar de un modo cómodo, rápido y eficaz por el ciberespacio, pero no es ni mucho menos el único modo de hacerlo. Siempre existe la posibilidad de ignorar los filtros y la personalización y buscar información más allá de las ya adquiridas inquietudes personales. Debería ser responsabilidad de la persona mantenerse informado, contrastar esa información y las opiniones que pueda encontrase sobre los motivos del intento de golpe de estado en Turquía.

Que los resultados de búsqueda de un usuario que se dedique a la cría de ganado estén relacionados, en mayor medida, a sus búsquedas anteriores y que no le aparezcan resultados sobre información que nunca ha buscado, eso no significa que éste en el futuro no pueda tener algún tipo de interés en la venta de vacas para coches. Internet no ha sido creado para, ni su estructura consiste en, hacer más curiosas a las personas. Su función es proporcionar la información que busca el cibernauta en un momento concreto. Es cierto que puede ayudar a compartir puntos de vista, a ampliar intereses y

---

61 http://www.wsj.com/articles/SB10001424052748704901104575423294099527212 Consultado el 25 de agosto de 2016.

conocimiento entre los usuarios pero son ellos mismos los que tienen que ser abiertos de mente, curiosos y estar motivos para aprender cosas nuevas.

Pariser muestra cómo la burbuja filtro opera en todos los ámbitos de la red y también en las redes sociales y pone como ejemplo la personalización del muro de Facebook. Se advierte que cuanto más se responda a opiniones dejadas en el muro de Facebook de un amigo, más relevancia tendrá ese amigo en el muro propio y más tiempo y más arriba aparecerán sus comentarios. A medida que se deje de reaccionar ante sus comentarios su aparición en el muro será menor hasta llegar a no aparecer.

A pesar de que los argumentos sobre las limitaciones que supone la burbuja filtro tienen una base muy sólida y fundamentada, también es cierto que hay algo, concretamente en el contexto de las redes sociales, que parece que el autor ignora o al menos no contempla es su argumentación. La primera definición explícita sobre red social se encuentra en la literatura antropológica de la mano de John Barnes. Así se explica respecto a la red social,

> Cada persona está, por decirlo de alguna manera, en contacto con un número de personas, algunas de las cuales están en contacto entre sí y otras no [...] Me parece conveniente hablar de "red" para referirnos a un campo social de este tipo. La imagen que tengo de ello es la de un conjunto de puntos, algunos de los cuales se unen por líneas. Tales puntos son las personas o, a veces, los grupos, y las líneas indican interacciones entre las personas.
> (Barnes, 1954, p 43)

Lo novedoso de este punto de vista para la antropología era que las relaciones sociales podían no estar sometidas a las reglas de parentesco, de clase, de situación geográfica, etc., como proponía el análisis del estructuralismo funcionalista imperante en la época. Esta nueva perspectiva suponía que ego (el actor, en el caso de esta investigación el usuario) tenía relaciones con otros egos que, a su vez, tenían relaciones que podían estar o no conectadas entre sí y que ego, podía, en cierta medida, manipular su red social según sus intereses.

Este planteamiento entiende que esas redes sociales son móviles y que en cada momento y cada situación la red puede verse modificada por un amplio número de razones. De este modo, no se ha

de suponer que el hecho de formar con una serie de individuos una red social en un momento determinado implique necesariamente que esa red social permanezca en el tiempo. Los cambios en las conexiones entre miembros de esa red social inicial pueden llevar a la desaparición total de un miembro, de varios o de la red misma, sin que ello suponga ningún inconveniente o situación problemática. Lo mismo se puede decir de las redes sociales digitales. La desaparición de un contacto en el muro de Facebook no supone para la red social más que una transformación natural debido al cambio de conexiones de la red. Esta desaparición es una consecuencia, en un sentido antropológico, natural de la pérdida de lazos entre los diversos egos.

> También en una red social pueden existir vínculos potenciales. Es decir, no todos los vínculos que una persona pueda tener tienen que estar activados en todos los momentos. Estos pueden permanecer durante un tiempo indeterminado en estado latente hasta que llegue el momento de ser necesitados para alguna acción social.
> (Requena Santos, 2003, p. 147)

Otra cuestión que parece no haber tenido en cuenta Pariser sobre Facebook es pensar que ésta, como la red social física, es una herramienta socializadora. Si bien es cierto que esta plataforma se presenta como un modo de conectar a la gente, y que a través de ella es fácil estar informado sobre los movimientos de las personas que pueden estar alejadas entre sí, esto no significa que éstas vayan a mantener y/o mejorar sus relaciones sociales. Si alguien es amigo de una persona pero ésta no aparece en su muro, debido a que sus intereses están alejados entre sí, no parece que esto sea un problema ya que en las redes sociales físicas sucedería lo mismo por una tendencia hacia la afinidad. Por otra parte, son las personas las encargadas de hacer que los lazos que las unen sean lo suficientemente fuertes como para que no desaparezcan de su muro de Facebook, pues como afirmaba Aristóteles *"*la amistad forma parte de las cosas estables*"* (Aristóteles, *Ética Nicomáquea* VII, 1238a).

Culpar a la personalización y a la experiencia del usuario de que las personas no sean más curiosos e inquietas y que no utilicen Internet y las redes sociales para desarrollarse y desarrollar relaciones sociales es una visión paternalista por un lado, en la medida en que se considera al individuo incapaz de evolucionar y avanzar por sí mismo e infantil por el otro, ya que se culpa a la personalización y la experiencia del usuario de la propia falta de inquietud. Al fin y al cabo, ambos

aspectos se han generado a base de información que se le va dando a los algoritmos para que muestren al usuario aquello por lo que está interesado.

Se considere útil o no o se considere un freno para el desarrollo personal, es necesario, tanto para la experiencia del usuario como para la personalización de contenidos, recabar datos personales para su correcto funcionamiento. Sin información relativa a lugar geográfico desde que se conecta el usuario, su profesión, su estado civil, su género o sus aficiones, ambas herramientas serían menos precisas a la hora de realizar su función y es probable que los usuarios demandasen estas herramientas, pues si nos las quisieran y no las usaran no se hubieran implementado tan bien en el uso cotidiano de Internet.

Se puede considerar que esta información es necesaria para la contextualización de la información que el buscador debe mostrar al usuario. Si se realiza una búsqueda sobre "playas" desde un dispositivo en Barcelona, es muy probable que se estén buscando playas cerca de la ciudad condal y no playas del sur de Andalucía. Si después se introduce la búsqueda "chiringuito" el algoritmo calculará que habiendo realizado una búsqueda sobre playas estando en Barcelona lo más lógico es mostrar resultados relativos a "chiringuitos de playa en Barcelona". El algoritmo realiza con precisión, con la información disponible, su función.

Ahora bien, parece que entre los críticos de la personalización y los defensores de la privacidad, este hecho no es relevante a la hora de exponer sus argumentos. Estos resultados, que hacen de Google una herramienta muy bien valorada por su eficacia a la hora de devolver resultados óptimos, están basados en la información que se recoge y almacena del usuario. Sin el acceso a esa información sobre los individuos, el buscador sencillamente no funcionaría como lo hace hoy en día, esto es, dando respuestas exactas a preguntas concretas realizadas por los usuarios. Los argumentos para criticar la falta de privacidad que tienen los usuarios de Google no parecen tener en cuenta que el éxito del buscador radica precisamente en el uso de información personal de los usuarios. Resultaría difícil para el buscador mostrar resultados certeros sin contextualizar la búsqueda. Siguiendo con el ejemplo, sería como preguntar a una persona "¿playa?" en vez de "¿conoces algún chiringuito","¿quieres ir a la playa?" o "¿conoces alguna playa cerca?".

5.1.3 Comercio electrónico

En el año 2013, sólo en España, más de 11 millones de personas habían realizado algún tipo de compra por Internet[62]. Según la Asociación española de economía digital, el comercio electrónico en España había crecido en 2015 un 20% respecto al año anterior, situándose en los 20.000 millones de euros[63]. A nivel global, este tipo de comercio suponía ese mismo año casi el 6% del comercio total mundial[64]. Estas cifras ponen de manifiesto la importancia del ciberespacio como espacio económico y mercado global. En un entorno, de por sí ya competitivo, las campañas de marketing, el llegar y acertar con el público objetivo, minimizar gastos y aumentar beneficios es una cuestión fundamental para las empresas.

Antes de la llegada de las tecnologías digitales, las campañas de publicidad eran lanzadas para el público en general. Si bien es cierto que se podían marcar criterios, como determinar en qué tipo de publicaciones se anunciaba un producto, a qué horas se emitía determinado anuncio para llegar al púbico deseado, en qué épocas del año se realizaban determinadas campañas, etc., lo cierto es que las empresas necesitaban presupuestos elevados en campañas de marketing para llegar a un público que podía, o no, ser el público objetivo de sus productos, con la confianza, a veces ciega, de acertar y llegar al consumidor esperado.

Actualmente el comercio digital y el marketing en línea disponen de mecanismos mediante los cuales pueden dirigir sus estrategias hacia un consumidor más concreto, donde concreto significa aquí más, en principio, interesado en los productos que venden esas empresas. Estas compañías, junto con las estrictamente tecnológicas, son las que forman el conjunto de usuarios que se han denominado productores/usuarios. Son éstas las que hacen uso de determinados servicios que ofrece Google, que se han enumerado y explicado en páginas anteriores y que tienen como prioridad para vender sus productos el disponer de información relativa a los hábitos de vida, de navegación por la red y de consumo de los cibernautas. Estas herramientas están dirigidas principalmente a que las empresas puedan realizar sus negocios de un modo rentable.

---

62 Datos extraídos del Instituto Nacional de Estadística. Véase http://www.ine.es/ss/Satellite?L=es_ES&c=INECifrasINE_C&cid=1259943296411&p=1254735116567&pagename=ProductosYServicios%2FINECifrasINE_C%2FPYSDetalleCifrasINE

63 https://www.adigital.org/?noticias=record-crecimiento-del-comercio-electronico-2015-20-000-millones-euros

64 http://www.emarketer.com/Article/Retail-Sales-Worldwide-Will-Top-22-Trillion-This-Year/1011765

Mediante el uso de herramientas que Google pone a disposición de las empresas, éstas pueden saber a qué tipo de consumidor/usuario deben dirigir sus campañas. A través del análisis de datos de los usuarios, saben qué tipo de consumidor es su público objetivo, cuándo tienen que realizar campañas, en qué medios, bajo qué criterios, etc. Google dispone de información valiosa sobre los hábitos de vida de las personas usuarias de sus servicios. Información que como se ha visto puede ser dada directamente por el usuario o conseguida mediante el modelo de usuario, la experiencia del usuario y a través de la huella digital que éste deja mientras navega por la red.

Los servicios y las herramientas que Google ofrece a los consumidores/usuarios, aquellas herramientas que hacen que la experiencia del usuario sea lo más satisfactoria posible, son de uso gratuito. Servicios como SafeSearch, Google Instant, los servicios de Google Maps, el correo electrónico de Gmail, YouTube, Google+, etc., no suponen ningún coste monetario para el usuario, tan sólo, como se ha mencionado más arriba, es necesario en algunos casos el registro para tener acceso a los servicios.

El registro y el propio uso de estos servicios supone una fuente importante de información, que como Google mismo informa, recaba, almacena y gestiona. En este sentido, se puede interpretar que en cierta medida es el propio usuario, al aceptar las condiciones de uso y al utilizar los servicios de la empresa, quien, de algún modo, ofrece la posibilidad a Google, a través del consentimiento, de hacer uso de sus datos. Pero no todos los servicios de Google son gratuitos. Las empresas, que desean tener acceso a la información que aquélla tiene sobre los consumidores/usuarios, deben pagar por tener acceso a esa información que, como se ha dicho, será vital para dirigir sus esfuerzos de un modo rentable.

Servicios como Google Analytics, que gestionan la información sobre el tráfico en una página web, Google Adwords que permite la inclusión de anuncios patrocinados en los resultados de búsqueda o Google Adsense, que incluye publicidad relevante dentro de los sitios web, tienen un coste para las empresas que quieren comprar esos servicios. No disponer de visibilidad en Internet es para una compañía una pérdida de púbico potencial y supone estar en una situación de desventaja respecto a sus competidores con presencia en la red. De ahí la importancia que una empresa disponga de una página web en primer lugar y que pague por alguna de las herramientas de análisis de datos que ofrece Google.

El esquema puede realizarse del siguiente modo. Google ofrece servicios a sus usuarios, ya sean consumidores o productores. Para los primeros, las herramientas y los servicios de la compañía son gratuitos, siempre afirmando que aquéllos están pensados para reforzar una buena experiencia del usuario. Mediante estos servicios Google accede a información que luego podrá gestionar para sus otros clientes, los productores. Éstos, las empresas, tienen que pagar un coste por acceder a estos servicios que les dará acceso a determinada información de los consumidores. No será información personal de los usuarios, pero sí datos suficientes como para saber cómo tienen qué gestionar sus recursos para realizar el mayor número de ventas, o más exactamente, cómo obtener el mayor beneficio de ellas.

Estas empresas recuperarán su inversión cuando el usuario realice una compra. Podría parecer que recuperar la inversión realizada no resulta tan fácil, en la medida en que no todos los usuarios que vean el anuncio de un producto lo acabarán adquiriendo. Pero hay que tener en cuenta el valor de tráfico y la relevancia. La visibilidad de un anuncio no determina las ventas finales pero el llegar a un mayor público aumenta las posibilidades de realizar efectivamente una venta. Así mismo, a medida que los usuarios clican en un anuncio y son redirigidos a una página web concreta, ésta gana relevancia lo que significa a su vez una mayor visibilidad.

La importancia de la relevancia y el modo en que las empresas pueden ganar dinero por el simple hecho de su presencia en Internet puede verse en los buscadores especializados donde son los propios usuarios los que pueden puntuar a las empresas. Estos buscadores, como pueden ser TripAdvisor o Booking por poner unos ejemplos conocidos, permiten a los usuarios puntuar las empresas incluidas en ellos, como restaurantes, hoteles, atracciones, etc. Cuanto mayor sea la puntuación dada por los usuarios, más alta será la posición en la que se encuentren. Si se está realizando una búsqueda sobre restaurantes en Barcelona, el buscador especializado mostrará primero el restaurante mejor valorado por los usuarios, mostrando no sólo en qué posición está en términos absolutos a todos los restaurantes de la ciudad, sino que también mostrará opiniones escritas por los usuarios, fotos que hayan podido realizar éstos, datos de interés del local, etc. No todas las personas que vean el restaurante número uno en el ranking se decidirán por ir a él, pero lo cierto es que todos los usuarios que busquen un restaurante en Barcelona verán el negocio que está el número uno y difícilmente verán el que está en la posición cien o mil. Así funciona la relevancia en Internet, de este modo es fácil entender la importancia de ésta para las empresas y los negocios en línea.

Un ejemplo más para mostrar la importancia del comportamiento del usuario/consumidor. Éste dispone información relativa a su situación geográfica, que mediante la IP puede situar en España. Google por su parte vende esa información a las empresas en forma de servicios para que éstas puedan adecuar su publicidad a las demandas del usuario situado en esa país. En este caso podrían ser mostrar la publicidad en un idioma concreto, anunciar determinados productos en función de la estación del año en la que se encuentre, adecuar los productos anunciados a las tendencias de ventas en este país, mostrar el precio del producto en función de la divisa que sea utilizada, el tiempo estimado de llegada del producto desde el país de origen, etc.

La importancia del comercio electrónico y la personalización de contenidos y publicidad, ha supuesto que surja la pregunta de quiénes son los verdaderos actores de la red y el ciberespacio. Algunas voces se han alzado para dar respuesta a esta pregunta, afirmando que el usuario-comprador, lejos de ser el actor al que se dirigen todas las acciones, es realmente el producto de Internet.

5.1.4. El usuario como producto

Al comienzo de esta investigación, al tratar la tendencia a pensar en Internet como un espacio sin lugar, libre y gratuito se había matizado esta última afirmación, observando que los usuarios (consumidores) además de realizar pagos relativos a los dispositivos utilizados para navegar por la red, la contratación del acceso a la misma, etc. hacían otros tipo de "pagos" que podían considerarse menos tangibles o monetarios.

El hecho de navegar por Internet de un modo gratuito, en el sentido de no tener que pagar para utilizar determinados servicios, visitar sitios web o contactar con amigos o familiares alejados geográficamente, no significa necesariamente que sea un acto libre de cargos. Como consumidores, los usuarios tienen que pagar de algún modo esos servicios y el modo en que lo hacen es a través de información relativa a sus movimientos en el ciberespacio. Las herramientas que permiten a los ciberciudadanos estar informados, comunicarse, jugar o comprar, están desarrolladas por empresas. Empresas que han invertido tiempo y dinero en la generación de esos servicios por un lado y que permiten a los usuarios realizar todas aquellas tareas que hacen de Internet un lugar amplio y lejanamente limitado en sus posibilidades.

Entre empresas como Google y aquellas denominadas usuarios-productores están los usuarios-consumidores. Ellos son el medio por el que ambos extremos consiguen ganancias. Google les ofrece unos servicios gratuitos a estos últimos con los que, en principio, no consigue beneficios. El negocio está en las empresas, que sí que pagan a Google por la información que dispone sobre los consumidores. Douglas Rushkoff expresa claramente lo que se está intentando afirmar aquí. Su ejemplo versa sobre la red social Facebook pero el ejemplo puede servir sin reparo en esta reflexión, en la medida en que está tratando el tema de la supuesta gratuidad de los servicios en Internet.

> Ask yourself who is paying for Facebook. Usually the people who are paying are the customers. Advertisers are the ones who are paying. If you don't know who the customer of the product you are using is, you don't know what the product is for. We are not the customers of Facebook, we are the product. Facebook is selling us to advertisers[65].

En 2013 la revista Forbes publicaba un artículo bajo el título: *"Google Users- You're The Product, Not The Customers*". En él se mencionaban las palabras del magistrado Paul Grewal, sobre el modo en que Google obtiene beneficios siendo una empresa que ofrece servicios gratuitos a los usuarios.

> By now, most people know who Google is and what Google does. Google serves billions of online users in this country and around the world... With little or no revenue from its users, Google still manages to turn a healthy profit by selling advertisements within its products that rely in substantial part on users' personal identification information... in this model, the users are the real product[66].

Estas afirmaciones, que podrían sonar excesivas, no hacen sino apoyar las preocupaciones de la ciberética por la privacidad y la intimidad de los ciberciudadanos. En la medida en que se estima que la información sobre el comportamiento del usuario es vendida a los intereses de las empresas se considera al usuario el producto de Internet.

---

65 http://www.wired.co.uk/article/doug-rushkoff-hello-etsy Consultada por última vez el 26 de agosto de 2016.

66 http://www.forbes.com/sites/benkepes/2013/12/04/google-users-youre-the-product-not-the-customer/#25524fa4c162

Si se atiende a una de las definiciones que ofrece la Real Academia Española para producto, según la cual éste es el *"caudal que se obtiene de algo que se vende, o el que ello reditúa"*[67] entonces es acertado afirmar que el consumidor/usuario, o al menos la información relativa a su conducta en Internet, es efectivamente el producto de la red, ya que es éste y la información que de él se obtiene lo que otorga beneficio económico al ciberespacio y en concreto a las empresas o usuarios-productores que en él operan.

Este hecho puede resultar incómodo y no ser aceptado como una afirmación válida, ya que las personas no deberían ser tratadas como productos, pero existen precedentes que ayudan a confirmar, o cuanto menos a considerarla desde cierta perspectiva, como una posibilidad. En primer lugar y el ejemplo más claro que puede surgir acto seguido a tal cuestión es la esclavitud. Durante mucho tiempo la esclavitud se consideró, no sólo un tipo de sistema de producción sino, en muchos casos un derecho e incluso un hecho natural, como afirmara Aristóteles en su *Política*. Hicieron falta siglos para que finalmente se aboliera la esclavitud como un método común de fuerza de producción. Incluso hoy en día todavía puede hablarse de esclavitud y de trabajos forzosos, por lo que la idea del ser humano como producto no es ajena a éste.

Otro aspecto a tener en cuenta a la hora de abordar la idea del usuario como producto es compararlo con otro tipo de formas de vida que se han tenido hasta hace poco, y que en muchos casos todavía se consideran, como un producto para el beneficio y el consumo, es el caso de los animales no humanos. Ya sea para la experimentación, la fabricación de vestimenta o el consumo, lo cierto es que los animales no humanos han sufrido la desprotección y la falta de derechos, tratándoles como simples objetos para el consumo, esto es, como productos.

Estos dos ejemplos ponen de manifiesto que la idea de observar al usuario como un producto no es algo alejado de una práctica, hasta hace poco, habitual. Con esto no se pretende justificar que los usuarios sean tratados como esclavos o que no tengan derechos como no los tuvieron los animales no humanos. Lo que aquí se intenta señalar es que aunque las tecnología digitales, e Internet poco a poco están dejando se ser algo nuevo, y a medida que pasa el tiempo hablar de nuevas tecnologías se mantiene tan sólo como denominación (e incluso esto cada vez menos) es importante entender que la ética del ciberespacio y en consecuencia los derechos de los cibernautas son todavía caminos por recorrer. Hace falta seguir pensando, criticando, evaluando y avanzando hacia un ciberespacio

[67] http://dle.rae.es/?id=UH9P99t

que permita a todas las entidades que la conforman ajustar sus intereses hacia un bien común, sin que unas partes estén sometidas o supeditadas a los intereses de otras.

Google, en este sentido, aunque pueda parecer lo contrario, merece la atención sobre los esfuerzos que realiza para que este, aquí sí, nuevo orden del ciberespacio tenga lugar. No se trata de defender a la empresa alegando que el tratamiento que hace de los datos de sus usuarios siga una ética basada en el respeto por la privacidad y la intimidad de los mismos. De hecho, muchos de los usos que hace de los datos de sus usuarios pueden ponerse en tela de juicio y deberían ser mejorados.

Por otra parte es necesaria una claridad sobre qué significan datos personales, de qué tipo de usuarios está hablando en cada momento, a qué tipo de usuario está dirigida su Política de privacidad etc. Lo fundamental ahora y sobre esta empresa es entender en qué momento de la historia del ciberespacio se encuentra y cuáles son las herramientas, normativas, legales, sociales, éticas, etc., de las que dispone y disponen los cibernautas para llevar a cabo un ciberespacio ético y justo para todos sus miembros.

Hay que tener presente que esta idea del usuario como producto tienen sus fundamentos, en la medida en que él y su información es la moneda de cambio del ciberespacio. Sin embargo, no estaría de más abordar varios aspectos que pueden llevar a entender cuáles son las circunstancias de este producto y a replantearse tal denominación. Se puede atender a las múltiples formas en las que los ciberciudadanos están protegidos en el ciberespacio y que le alejan de esta idea de ser el producto real de la red.

En primer lugar están las leyes que cada país de forma individual o en conjunto en forma de organizaciones que los representan están llevando a cabo al respecto. El derecho a la privacidad es un derecho protegido por la mayoría de los países y una necesidad para formar parte de la Unión Europea, por ejemplo. La defensa de la misma no supone una novedad y se intenta proteger también en el ciberespacio. Aunque como se verá más adelante a veces no resulta tan positiva y/o beneficiosa como se pretende en un primer momento.

Por otra parte, las empresas tecnológicas son conscientes de la importancia de la privacidad para sus usuarios. En algunos casos han sido llevadas ante los tribunales precisamente por no querer ceder

ese derecho ante las autoridades. El caso de Apple en San Bernardino[68] o de Facebook en Brasil[69] han sido tal vez los casos más sonados durante el 2016. Así mismo, y como se ha dicho anteriormente, las mayores compañías tecnológicas tienen, de un modo explícito, políticas de privacidad donde se informa a los usuarios de sus derechos y el modo en qué pueden hacer usos de ellos ante abusos relativos al uso de su información personal.

Pero sobre todo, y en respuesta a la idea de pensar en los usuarios como producto, hay un hecho que no puede pasarse por alto y que es necesario apuntar en este momento. Es la cuestión sobre los servicios gratuitos que los usuarios tienen a su disposición. Los usuarios disfrutan de esos servicios sin ningún coste económico. Pero eso no significa que sean gratuitos. Éstos pagan con la información que de ellos se almacena y se usa con fines lucrativos por parte de las usuarios-productores. No deberían considerarse productos en la medida en que ellos participan de esa economía recibiendo servicios por su información. Si bien es cierto que no reciben compensaciones económicas por los servicios que prestan al ciberespacio, como se ha visto propone Lanier (página 23), no se puede decir que no reciban nada a cambio. Lo que reciben son todas aquellas herramientas por las cuales pueden hacer el uso del ciberespacio que hacen actualmente. De hecho, si se entiende por usuarios-productores "aquellos cuyo uso de Internet retroalimenta el sistema tecnológico" (página 11) y es la información que generan los usuarios aquello que permite a las empresas y a Google operar en la red, bien podría entenderse a los usuarios-consumidores también como productores del ciberespacio. Lo que haría que hablar del usuario como producto fuera incorrecto.

Algunos podrían afirmar que lo que reciben no compensa las pérdidas de derechos y de privacidad. Sin duda esto puede ser cierto, sobre todo en el modelo actual, tanto en el plano económico como ético. En primer lugar, y empezando con el segundo caso, está la cuestión que se ha avanzado anteriormente del concepto mismo de privacidad, que dificulta el avance en la comprensión de la información en el ciberespacio. Un concepto que no tiene en cuenta o desestima la importancia de la gestión de la información como mecanismo fundamental del funcionamiento de la red. Una vez revisado y renovado el concepto de información personal y privacidad, redefinido de modo que pueda haber una coexistencia entre el ciberespacio y la seguridad de mantener unas cuotas de

[68] http://www.bbc.com/mundo/noticias/2016/02/160225_tecnologia_apple_revertir_orden_fbi_desbloquear_iphone_ppb

[69] http://internacional.elpais.com/internacional/2016/03/01/america/1456855207_679012.html

privacidad con las cuales los individuos se sientan cómodos y seguros, tal vez el problema del uso de datos de los usuarios no sea de tal magnitud como el que se supone ahora.

En segundo lugar está la cuestión de la compensación por el uso que de se esa información se hace, una compensación que es ajena a quién produce la información pero netamente beneficiosa para quien la gestiona. La realidad es que, como la expresa Jaron Lanier, "hasta tal punto deseamos disfrutar de experiencias online gratuitas que aceptamos gustosamente no recibir ninguna compensación económica, ni ahora ni nunca, por la información que generamos" (Lanier, 2014, p. 47). Las personas desean servicios gratuitos, en cierta medida sin importarles cuánto coste informativo les está suponiendo. El uso de redes sociales, los servicios gratuitos de Google, la descarga online de productos protegidos, etc., son un claro ejemplo de esta falta de interés sobre el uso de información personal cuando se trata de navegar por la red gratuitamente.

La idea que esgrime Lanier y que ya se ha expresado es que cada individuo reciba una compensación por la información útil que éste pueda facilitar al ciberespacio, o dicho en sus propias palabras: "lo que pretendo es que las personas reciban el trato especial que merecen. ¿Cómo? Haciendo que reciban una compensación económica por la información que se obtiene de ellas si esta resulta valiosa" (Lanier, 2014, p. 39). Con un nuevo concepto de privacidad y una nueva economía de la información puede que las personas no se sientan tan desprotegidas o por lo menos se sientan compensadas ante una situación que ahora parece inclinarse de forma ventajosa hacia un único lado.

5.2. Política de privacidad de Google[70]

La política de privacidad de Google pretende mostrar a) qué datos son recogidos y los motivos de ese almacenamiento; b) cómo son utilizados y; c) el modo en que se puede acceder a esa información y cómo actualizarla. En términos cercanos a la ciberética, advierte a los usuarios sobre el acceso y el control sobre la información que generan en el ciberespacio y en concreto a través del uso de sus servicios y herramientas.

[70] Los datos recogidos en esta sección corresponden a la última versión publicada por el buscador con fecha a 28 de junio de 2016. Todas las citas de este capítulo, salvo que se especifique lo contrario, forman parte de la *Política de privacidad* de Google, que puede encontrarse en https://www.google.es/intl/es/policies/privacy/ por lo que no se utilizarán las citaciones regulares.

Siempre con el objetivo de "ofrecer mejores servicios a todos nuestros clientes" Google recoge y almacena información del usuario de varios modos. En primer lugar el modo más directo por el cual recoge información es la que se pide explícitamente para el uso de sus servicios. Muchos de éstos requieren el registro por parte del usuario para poder acceder a ellos. Así por ejemplo, para tener y activar una cuenta de correo Gmail es necesario ofrecer información personal. Por *información personal* se entiende nombre, dirección de correo, número de teléfono o tarjeta de crédito, "u otro tipo de datos que Google pueda relacionar de manera razonable con dicha información como, por ejemplo, los datos asociados a tu cuenta de Google*"*.

Un segundo modo por el cual Google recoge información del usuario es a través del uso que éste hace de los servicios de la empresa. En este caso no sólo se almacena información relativa a los servicios concretos que se utilizan sino también el modo en que se utilizan. Si se visualiza un vídeo de YouTube, Google almacena el vídeo que se ha visto, el tiempo que se ha estado viendo, esto es, si he ha acabado o dejado de ver, si se ha visto un anuncio o se ha cerrado o si las sugerencias de otros vídeos han sido atendidas. También se registra la entrada a sitios web donde la empresa haya vendido publicidad.

Es en este segundo caso, cuando el usuario hace uso de los servicios y herramientas, donde la empresa adquiere más información del usuario y donde las preocupaciones por la privacidad pueden tener mayor influencia. El motivo es que mientras se hace uso de sus servicios Google tiene la capacidad y el derecho, en la medida en que se han aceptado las condiciones de uso, de adquirir y almacenar información relativa al comportamiento del usuario mientras éste hace uso de sus servicios. Este control sobre el comportamiento del consumidor no es exclusivo del ciberespacio. Del mismo modo que al entrar en una tienda se anuncia al cliente de la existencia de circuitos cerrados de videovigilancia donde está siendo grabada todas las visitas de los clientes, Google hace lo mismo con los suyos, en este caso los y las cibernautas.

Durante el uso de sus servicios Google recoge información variada del usuario. Recoge información relativa al dispositivo desde el cual se está haciendo uso. La marca y modelo del dispositivo que se está utilizando; el sistema operativo y su versión; el IMEI del dispositivo, esto es, la "matrícula" que cada dispositivo lleva incorporada; la información sobre el proveedor de servicios y el número de teléfono. Además de esta información relativa al dispositivo Google almacena lo que denomina

“datos de registro”. Éstos se incluyen de manera automática cuando se realizan, por ejemplo, consultas a través del motor de búsqueda.

Estos “registros del servidor” serían: la web concreta que se busca; la dirección IP, proporcionada por el proveedor de servicios, que suele asignarse en función de la zona geográfica y que es individual para cada dispositivo; datos telefónicos, entre los que se incluyen el número de teléfono desde el que se hace la llamada y al que se hace la llamada, la hora y fecha de la llamada, la duración de la misma; otra vez el tipo de dispositivo; y las cookies. Las cookies, de las que se hablará más adelante, son pequeños archivos que se envían al dispositivo del usuario cuando se visita una web por primera vez. Cuando se vuelva a esa web, ésta tendrá información relativa al usuario, sobre cuándo fue la última vez que entró en la página, qué hizo en el sitio, cuánto tiempo estuvo en él, etc.

Además de la información del dispositivo y de los datos de registro, Google almacena información relativa a la ubicación física del usuario. Cuando se hace uso del servicio de, por ejemplo, Google Maps éste tiene que situar al usuario en un lugar determinado para poder darle coordenadas sobre su posición. Para ello se emplean la identificación de la IP, la posición por GPS, información sobre otros dispositivos cercanos y las antenas de conexión cercana.

Otro modo de recoger información es a través del uso de las cookies. Según la definición de Google,

> Una cookie es un pequeño fragmento de texto que los sitios web que visitas envían al navegador y que permite que el sitio web recuerde información sobre tu visita, como tu idioma preferido y otras opciones, lo que puede facilitar tu próxima visita y hacer que el sitio te resulte más útil. Las cookies desempeñan un papel muy importante, ya que sin ellas el uso de la Web sería una experiencia mucho más frustrante.

A través de estas cookies Google puede ofrecer a los sitios web información relevante sobre el tráfico que existe en su dominio. El usuario tiene cierto margen a la hora de aceptar o no la utilización de cookies, aunque debe ser consciente de que cabe la posibilidad que determinadas funciones o servicios no funcionen correctamente.

Estas son básicamente las formas en las que Google tiene acceso a los datos de los usuarios: información que se proporciona de forma directa para activar los servicios ofrecidos por la empresa; a través del uso que se hace de ellos; mediante datos relativos a la ubicación física del usuario y; el uso de cookies. Esta información sobre el uso de los datos personales está publicada de forma gratuita y accesible para todos los usuarios de Google y sus servicios. No es algo que la empresa intente esconder y tampoco parece que sea algo que ignore a la hora de lanzar un producto pues cada cierto tiempo la política de privacidad de la empresa se actualiza, atendiendo a las nuevas demandas de seguridad a este respecto.

El problema de fondo, que no el único como se verá más adelante, es la ambigüedad con la que se tratan determinados aspectos que tienen que ver principalmente con las cuestiones relativas al concepto mismo de usuario por un lado y en segundo lugar, y en relación a esto, los verdaderos sujetos o actores principales de Internet.

Al comienzo de esta investigación, y repetidas ocasiones, se ha mencionado la distinción realizada por Manuel Castells entre productores/usuarios y consumidores/usuarios. Se decía que se puede hacer una distinción entre aquellos actores del ciberespacio, los productores/usuarios, que se encargan de realizar la estructura del ciberespacio, de crear nuevas herramientas, productos y servicios para esos otros que denomina consumidores/usuarios. Éstos, en principio, no están involucrados en la construcción de la red, aunque cuando se ha tratado el tema del ciberactivismo se ha visto cómo son precisamente los usuarios los que, de un modo u otro, han creado nuevas formas de actuación en el espacio público digital y en esta medida se les puede considerar también como productores. Pero, salvo estas excepciones, sin intención de menospreciarlas, son una parte mínima de la construcción de Internet.

Es momento ya sí de analizar en qué medida Google respeta o no las posturas que la ciberética sostiene sobre la privacidad. Recapitulando, en el capítulo dedicado a la definición de la privacidad se han tratado varios aspectos de ésta que suelen tenerse como fundamentales para tratarla desde una perspectiva digital.

Se recordará que la idea principal era la de una privacidad basada en la información, que distinguía entre el espacio público y privado. También se ha dicho que mientras unas posturas le dan un valor intrínseco otras ponen el acento en el valor instrumental de la privacidad. Se ha definido la

privacidad como el control sobre la información o como acceso restringido a la misma. Por otra parte se ha visto una teoría que abarca las dos anteriores afirmando que la privacidad es una combinación de acceso restringido y controlado de la información. Así mismo se ha mostrado como las tecnologías digitales han hecho surgir una nueva forma de entender la privacidad, nueva en su extensión y alcance pero no en el fondo, que es la privacidad en público.

Por último, se ha presentado una privacidad basada en el conocimiento de información personal no documentada. Antes de comenzar con el análisis se adelanta aquí que Google, en mayor o menor medida, atiende a estas posturas que se analizarán a continuación cuando trata la privacidad de sus usuarios. En este sentido se verá cómo, lejos de ser una empresa que atenta contra la privacidad de los usuarios, intenta que éstos y su privacidad estén protegidos en el ciberespacio. El problema no será una cuestión de cómo Google gestiona esa información sino del modo en que funciona la red misma.

5.3. Google y la privacidad entendida como informacional

Como parte del ciberespacio, Google entiende la privacidad en términos de información. Como empresa tecnológica que almacena y gestiona la información de millones de internautas, ya sean productores/usuarios o consumidores/usuarios, sólo puede entender la privacidad en estos términos. Por si pudiera haber alguna duda, toda su política de privacidad está basada en la idea de dejar claro al usuario qué hace con su información. Desde el primer momento avisa que su política está basada en hacer entender al usuario cómo y para qué utiliza la empresa la información que recaba.

A medida que se avance en el análisis de la política de privacidad de Google y se compare con las diversas teorías, este carácter informativo de la privacidad se hará más evidente e inequívoco. Precisamente lo que inquieta a cibernautas y teóricos críticos con la empresa es precisamente la desinformación o ambigüedad a la hora de definir la cantidad y el uso que de ésta hace la empresa.

5.4. Google y el espacio público y privado de la privacidad

En este, el primer punto esencialmente de análisis, la cuestión sobre la distinción de dos espacios separados y diferenciados, el público y el privado, resulta ya de entrada una cuestión complicada de analizar. Se podría decir que Internet es, casi por definición, un espacio público. Un lugar donde las personas comparten información entre sí y un medio de comunicación. Las búsquedas de resultados en Internet parten de la idea de que otra persona ha puesto esa información al alcance público.

Las redes sociales o blogs son un claro ejemplo de espacio público donde las personas se dan a conocer y contactan entre sí, comparten información y ponen de manifiesto sus intereses y opiniones. Los juegos en línea tienen la característica principal de ser juegos de interacción social donde los jugadores, incluso alejados en el espacio, participan de un mismo juego o partida. Puede que no se conozcan personalmente, que nunca hayan estado en el mismo espacio físico y que hablen idiomas diferentes. Antes de la aparición de este tipo de juegos, era necesaria la presencia física de los jugadores en un lugar determinado para realizar las acciones. Ahora es posible una distancia espacial. Mientras unos pueden jugar desde sus casas, otros lo pueden hacer en un transporte público, en la playa, en la biblioteca, etc.

El intercambio de bienes y servicios y el comercio en general, han sufrido una transformación también en este sentido. Ya no es necesaria la presencia del vendedor o comprador en un lugar determinado, como tampoco lo es la del producto. El comercio electrónico ha supuesto un cambio sustancial en los modos de intercambio. Las tiendas físicas, los mercados, los productos seleccionados, etc., han dejado paso a un nuevo modelo económico donde es posible comprar casi cualquier cosa, de cualquier parte, en cualquier lugar. La comunicación, el ocio o la compra venta han sido, tradicionalmente, acciones llevadas a cabo en espacios públicos. La movilidad del comunicador, del jugador o comprador hacia un lugar donde desarrollar esas acciones era necesaria para realizar la tarea. Ahora, con las tecnologías digitales e Internet, ese cambio de espacio ya no es necesario.

Cada acto que se realiza por la red tiene un carácter público en la medida en que son relaciones sociales que, antes de las tecnologías digitales, se realizaban en espacios públicos, bibliotecas, escuelas o universidades para la búsqueda de información; plazas públicas, bares, clubes y asociaciones para la socialización; ludotecas o centros lúdicos para la diversión en grupo; omercados, tiendas, supermercados o centros comerciales para la compra de bienes y servicios. Las necesidades humanas, así como las relaciones sociales permanecen, es el medio en el que se llevan a cabo lo que ha cambiado. Y este cambio de medio ha propiciado la disolución del espacio, al menos el espacio diferenciado del resto de actividades.

La cuestión que parece preocupar cuando se trata de Google es que todas estas relaciones sociales, que antes se diseminaban en el bibliotecario o profesor que disponía de la información que se necesitaba, el camarero que sabía si se consumía un café con leche o un carajillo de coñac o el

tendero que podía conocer cuántas barras de pan se consumía a la semana, están ahora concentradas en una sola empresa.

Para realizar todas estas acciones, estas formas sociales, el individuo tenía que seguir toda una serie ritual que le hiciera pasar de un espacio a otro. Cambiar su vestimenta, adecuándola a las convenciones sociales que impedían o dificultaban salir a la calle con la ropa que se usa para estar en el espacio privado, arreglar su aspecto, tal vez lavándose los dientes y acicalando su pelo, calzándose adecuadamente para salir a la calle, aprovisionarse de dinero, llaves de casa, etc., bajar a la calle, acercarse hasta el establecimiento que más le conviniese para realizar la acción social determinada, relacionarse con otras personas y volver a casa.

Todo este ritual o conjunto de acciones para realizar la tarea así como el cambio de escenario entre la casa y los establecimientos reforzaban la idea de separación entre espacio público y privado. Estos pasos que se pueden reducir a tres: 1) hogar; 2) estado liminal donde el individuo se prepara para pasar de un estado a otro[71] y; 3) espacio público, han sido reducidos con las tecnologías a un simple estado de "estar". El individuo ya no tiene que pasar por el estado intermedio, aquél que le prepara para el cambio, para estar fuera o dentro, en un espacio privado o público.

Ahora se puede acceder al espacio público desde lo que antes se consideraba privado y a la inversa. Se puede charlar con amigos o hacer la compra desde la comodidad del hogar. Por otra parte, se puede disfrutar de la vida privada en espacios públicos como puede ser leer el correo personal. De hecho, siempre ha habido una convergencia entre vida privada y pública. Así, los chismorreos y cotilleos privados han estado siempre a la orden del día en los espacios públicos, o las puertas de las casas en determinadas zonas de las ciudades o las ventanas abiertas de par en par dando acceso al espacio privado desde lo público no han sido rarezas, al menos hasta que las conformaciones de las ciudades lo han permitido.

Parece como si esta ausencia de un lugar intermedio fuera el motivo por el cual el individuo siente una pérdida de privacidad y de invasión de su vida privada. No pudiendo controlar aquello que queda dentro o fuera de la zona de confort, no habiendo un estado que le permita preparase

---

[71] El estado liminal en antropología es utilizado para explicar el paso de un estado a otro dentro de la comunidad. Durante este espacio de tiempo, la persona no pertenece a ninguno de los estados anteriores y es un momento donde podría decirse que queda suspendida cualquier distinción. Este concepto es utilizado para explicar los ritos de paso dentro de las comunidades. Fue desarrollada en primer lugar por el antropólogo Arnold Van Gennep en su obra *The Rites of Passage* (1960).

mentalmente para cambiar de zona o situación, no sabiendo cuándo se puede relajar de la vida social, siente la necesidad de buscar un motivo para esa carencia. Google, utilizado casi como sinónimo de Internet por muchos usuarios, motor de búsqueda, responsable de la publicidad en línea, gestor de páginas web y controlador del tráfico en la red, está en todos los ámbitos del ciberespacio y utilizado por la mayoría de los usuarios, y como tal, es razonable tenerlo también como el causante de esa pérdida de estado intermedio.

La empresa, sin embargo, no es sino la cara más visible de todo el entramado de tecnologías digitales que han disuelto ese estado liminal. Atendiendo a su "Política de Privacidad" no puede decirse que exista ninguna intención explícita de acabar con las esferas públicas y privadas. Su objetivo es ofrecer herramientas y servicios a todos sus usuarios, usuarios que por otra parte una vez han entrado en el ciberespacio lo harán ya sin esa diferencia de espacios, la pérdida entonces es anterior al uso de los servicios de la compañía.

Ahora bien, como empresa de Internet, es ventajoso para ella que las personas sean en todo momento cibernautas. La vida fuera de la red no aporta ningún beneficio para Google y todo lo que se realice lejos de su control le supone una pérdida de posibilidades. De ahí que dirija sus esfuerzos en el lanzamiento de productos y en la promoción de la vida en línea.

Google debe entenderse como lo que Javier Echeverría denomina "señores del aire". La construcción del ciberespacio, del tercer entorno, no está en manos de los ciberciudadanos o telepolitas sino por aquellos usuarios-productores que lo construyen.

> Puesto que la red es costosa y tiene fama de insegura, los señores neofeudales ofrecen protección a sus telesiervos, garantizándoles que sus problemas estarán resueltos por el señor correspondiente si se mantienen fieles a la empresa que les proporciona el acceso a E3 (tercer entorno).
> (Echeverría, 1999, p. 181)

Si la ciberética desea mantener estos dos ámbitos separados deberá dirigir sus esfuerzos en encontrar un discurso dirigido al usuario. Al fin y al cabo, es éste quien se ha alejado de tal separación. Mediante el uso de dispositivos que le permiten una mayor movilidad y conectividad al mismo tiempo y haciendo uso de las herramientas que le permiten compartir su vida privada en

público, es el usuario el que está disolviendo ambos espacios. No es una cuestión tecnológica, sino social. No se trata de imponer el mantenimiento de ambos espacios separados, sino de observar, analizar y tratar en consecuencia si los individuos y la sociedad en general, quieren todavía mantener esa división. Evidentemente las empresas productoras de Internet tienen sus intereses en que estos espacios se disuelvan, en la medida en que dispondrán de unos consumidores siempre conectados.

5.5. Valor intrínseco y valor instrumental de la privacidad en Google

En su momento se ha mostrado cómo los diversos autores y autoras entienden y ponen el acento del valor de la privacidad en diferentes aspectos. Mientras unos la entienden con un valor intrínseco, otros no ven en ella más que un valor instrumental para alcanzar cualquier otro fin. Sin embargo, en mayor o menor medida, todos tienden a considerarse con cierto valor instrumental-

A modo de resumen, como se recordará se decía que para Stanley Been la privacidad es el medio por el que se crean relaciones de respeto. Por su parte, para Charles Fried la privacidad era necesaria para desarrollar relaciones de amor, amistad o fraternidad. James Rachels consideraba la privacidad como necesaria para el establecimiento de relaciones sociales diferenciadas. En este sentido, es el grado de privacidad de las relaciones lo que determina las relaciones fraternales de las laborales o de las amorosas. Se había mostrado como Deborah Jonhson, en un intento de acabar con la dicotomía entre valor en sí mismo o valor vehicular para alcanzar un fin, entendía que la privacidad es impensable sin la autonomía. Si la autonomía tiene un valor intrínseco y ésta está sujeta a la existencia de la privacidad, esta última tiene que ser también considerada como un fin en sí misma, en el sentido de condición necesaria de aquélla.

Antes de comenzar el análisis sobre cómo entiende Google, en términos de valor, la privacidad, es necesario hacer un apunte relativo a las propuestas de las ideas antes mencionadas. En primer lugar cabe preguntarse sobre estas relaciones sociales que, desde el punto de vista de los autores antes mencionados, dependen o están mediadas por la privacidad que versa entre ellas.

Parece existir en estos argumentos una confusión entre los conceptos de privacidad e intimidad. Confusión que puede encontrarse en Deborah Jonhson cuando trata el valor intrínseco e instrumental de la privacidad. Esta autora trata ambos conceptos como sinónimos y los utiliza indistintamente para sus argumentos (Jonhson 1984, p. 119). Pudiera parecer que ambos conceptos

efectivamente pueden tenerse como sinónimos, ya que la intimidad está relacionado con aquello privado. E incluso podría suceder que los matices, que suceden en la lengua española no existan en la anglosajona. Lo cierto es que, si bien en el uso habitual de los conceptos éstos pueden no estar bien diferenciados, tanto el Oxford Dictionary como el Cambrigde Dictionary tiene acepciones diferentes para ambos conceptos. Del mismo modo que sucede con los de lengua hispánica.

El concepto de íntimo tiene que ver con aquello interior de cada persona, se dice también de una amistad o de una relación. Es aquello que está reservado a una persona o conjunto de personas, como puede ser la familia o una relación amorosa. Sus definiciones tienen que ver, efectivamente, con los modos de relaciones sociales que se desarrollan entre las personas. La privacidad, sin embargo, tiene que ver con aquello que no se realiza a la vista de todos, aquello que es particular en tanto no perteneciente a lo público, es lo relativo a la vida privada de las personas.

Si bien ambos conceptos están muy cercanos, en la medida en que las relaciones íntimas forman parte de la vida privada de las personas y en tanto ésta forma parte de aquello que suele estar protegido por la privacidad, esto no significa que sean sinónimos. Del mismo modo que tampoco puede derivarse de la importancia de las relaciones íntimas el valor instrumental o intrínseco de la privacidad. Incluso si las relaciones íntimas, como pueden ser las relaciones de respeto que apunta Been o las relaciones de amor o fraternidad de Fried, fueran consideradas con un valor intrínseco este tipo de relaciones no necesitan, en tanto condición necesaria, de la privacidad para desarrollarse. Es totalmente plausible imaginar una relación íntima sin que exista privacidad en ella, pues una relación íntima es tan sólo una relación estrecha y cercana y no una relación opaca y secreta.

Más aún, si se adoptara la postura de afirmar la necesidad de la privacidad para desarrollar relaciones íntimas quedaría todavía la cuestión de si éstas tienen en efecto un valor intrínseco en sí mismas. Desde la teoría funcionalista de la antropología se podría afirmar que ambos tipos de relaciones sirven para mantener la estructura social. Las primeras en tanto permiten la vida en comunidad de forma armoniosa. Las segundas porque son el mecanismo que ayuda a la perpetuación de la especie. En este sentido, no tendrían un valor intrínseco sino un valor instrumental. Podría seguir afirmándose el valor intrínseco de este tipo de relaciones en la medida en que son parte esencial del sistema que mantiene la estructura social. Pero entonces, cabría preguntarse igualmente por qué es necesaria una privacidad para conseguirlas.

Dicho esto, atendiendo a que la intimidad y la privacidad no son lo mismo, viendo que la intimidad se refiere a las relaciones sociales que se pueden denominar relaciones personales y que la privacidad se refiere a aquello relativo al ámbito particular, resta analizar en qué medida entiende y atiende Google a la privacidad. Unas líneas más sobre la intimidad dejarán el espacio despejado para tratar con rigor la cuestión del valor intrínseco e instrumental de la privacidad centrado en esta empresa.

Google es una empresa de Internet que ofrece servicios a sus usuarios. Su objetivo principal es ofrecer estos servicios de un modo "gratuito" en términos económicos pero con la contrapartida de disponer de información de sus usuarios de modo que pueda lucrarse mediante la gestión de esa información. Como se ha dicho, la intimidad tiene que ver con el tipo de relaciones personales entre personas. Así habría que decir que a mayor grado de acciones exclusivas entre individuos mayor es su grado de intimidad.

Es cierto que Google puede tener acceso a información sobre las acciones y modos de esas relaciones íntimas y que, mediante la gestión de esa información puede disponer de información desconocida fuera de los márgenes de esa relación. Pero también es cierto que el acceso a la misma no disminuye el grado de intimidad entre las personas. Que una pareja se envíe correos electrónicos, imágenes o que busquen hoteles a través de Google Maps y que la empresa tenga acceso a esa información no implica que ese mail, imagen o búsqueda deje de ser íntima para las personas.

Podría argumentarse que, efectivamente, la intimidad de esa relación no está comprometida pero sí lo está la privacidad. Ahora bien, a este argumento se pueden encontrar al menos un contraargumento principal. Éste tiene que ver con el carácter visible y público de las relaciones íntimas. Las relaciones íntimas no son, casi se podría decir que por definición, privadas. De hecho, una parte fundamental de las mismas estriba en hacer evidente precisamente esa diferencia de la relación respecto al resto de individuos que rodean a las personas involucradas en ese tipo de relación. Cuando James Rachels afirma la necesidad de la privacidad para el desarrollo de relaciones sociales diferentes está afirmando precisamente esa visibilidad pública y social de la intimidad entre personas que organiza la vida social en diversas relaciones sociales. De este modo se podría afirmar que las relaciones íntimas no son privadas, sino bien al contrario públicas. Si esto es así no podría concebirse la pérdida de privacidad en una relación íntima en la medida en que ésta no participa de la privacidad.

Sin profundizar más en este aspecto de las relaciones íntimas es momento de analizar en qué medida Google considera la privacidad como un valor intrínseco o un medio para conseguir un fin. En un primer momento y como resumen de lo que se expondrá a continuación se puede decir que entiende la privacidad tanto como un valor intrínseco como uno instrumental. Puede resultar paradójica e incluso contradictoria esta afirmación pero la intención de los argumentos que se expondrán a continuación pretenden clarificar esta idea y disolver las posibles contradicciones.

La base del negocio de Google es la gestión de la información de los usuarios. En el estado actual del ciberespacio, toda esta información se considera de carácter privado, a no ser que el propio usuario la haga pública. Las opiniones, los comentarios, los perfiles en las redes sociales, etc., son considerados como información pública de los usuarios y en principio no parece existir ningún conflicto con la privacidad en este sentido.

Existe, sin embargo, otro tipo de información que el usuario y la ciberética considera como sujeta a las reglas de la privacidad. El dispositivo, el lugar o la hora de conexión, el tiempo de conexión, las visitas a sitios web y todo aquello relacionado con el tráfico web, forman parte de ese tipo de información que parece necesitar la protección de la privacidad. Pero lo cierto es que se utiliza el móvil o la tableta en espacios públicos, se hace uso de conexiones wifi públicas y se navega por la red desde bibliotecas, bares, plazas y demás lugares de acceso público donde cualquier persona puede acceder a esa información. Es el propio usuario el que hace pública esa información desde el momento en que las acciones se llevan a cabo en espacios públicos.

Sí existe otro tipo de información de carácter tradicionalmente privado a la cual tiene acceso Google, como pueden ser datos personales, datos bancarios, correos electrónicos, acceso a documentación en línea de los usuarios, etc. Estos datos que tienen carácter de confidenciales se diferencian de otro tipo de información que también puede ser considerada como confidencial o privada y que tiene que ver con la vida "social" del usuario en el ciberespacio. Esta información está relacionada con las búsquedas realizadas en el buscador, la conexión a redes sociales, las compras realizadas, etc.

Google tiene acceso a mucha de la información del usuario contenida en el ciberespacio. Como motor de búsqueda, indexador de información en la red, vendedor de publicidad en línea, controlador del tráfico en Internet, red social, proveedor de correo electrónico, almacén de

información en la nube o líder en dispositivos móviles, Google dispone de una información ingente de información. Ese acceso a información es su ventaja pero también su debilidad. Debilidad porque le pone en el punto de mira de toda crítica que haga referencia al uso de información en el ciberespacio. Ventaja porque es esa custodia de la privacidad de los usuarios lo que hace estar por delante del resto de empresas, buscadores y demás "señores del aire" del ciberespacio. Es precisamente estas dos situaciones las que hacen que atienda a la privacidad tanto como un fin en sí mismo y como un medio para alcanzar otros propósitos.

En su Política de privacidad, Google hace hincapié en la importancia de la privacidad de la información de la que dispone. Si bien es cierto que su política contiene algunos vacíos conceptuales o argumentativos, también es cierto que su mayor preocupación, ya sea por una cuestión ética (donde se hablaría de la privacidad como fin) o una estrategia empresarial (valor instrumental) es dejar claro qué tipo de uso hace de la información gestionada de sus usuarios. El valor como fin de la privacidad en Google viene determinada por la naturaleza misma de la empresa. Su producto esencial es la información, es aquello que produce, gestiona y vende. Si la información de los usuarios fuera accesible para todas las empresas que operan en Internet, Google no tendría nada con lo que obtener beneficios ya que tampoco tendría nada que ofrecer a los usuarios-productores.

Del mismo modo que cualquier otra empresa que cuida del producto por el cual después obtendrá sus ganancias, Google cuida de su mercancía, que en su caso es la información de sus usuarios. La existencia de la privacidad en el ciberespacio es importante para Google en la medida en que es la base de su negocio, el producto que luego podrá vender y del cual sacará beneficios. El éxito de Google radica precisamente de la existencia de la privacidad en el ciberespacio, en que dispone de una información especial dentro de éste, especial porque no es accesible para todo el mundo. Es el acceso a este tipo de información la que le permite actuar, a día de hoy, como actor principal de la red, haciendo que sea el señor de los señores del aire.

Internet es básicamente un espacio informacional. Su objeto principal son los datos y su base es la generación, almacenamiento y transmisión de información. Por lo tanto para cualquier actor de la red la información es igualmente básica e importante. Con independencia de los motivos por los que se use Internet, ya sea para aprender, jugar, generar beneficios o cualquier otro tipo de acción en el ciberespacio, la información es, podría decirse, el lenguaje de red. Nada existe en este espacio

que no sea informativo. De ahí que tanto para un usuario medio, para una tienda de calzado o para Google el carácter informativo del ciberespacio es esencial, aunque sea por motivos diferentes.

En este sentido se puede afirmar que en la medida que la red *es* gracias a la información ésta tiene un valor intrínseco para aquélla, pues sin información el ciberespacio sería un lugar vacío. Sin información no podría darse esa conexión entre nodos que permite el intercambio y el movimiento de datos que es lo que constituye el ciberespacio. La existencia y posesión de una información diferente, que por diferente se debe entender aquí privada o al menos no accesible a todos los agentes que intervienen en la red, hace que Google se distinga del resto de actores. La privacidad en este sentido es básica para la existencia de Google, de ahí su valor intrínseco.

Aquí, algunos podrían afirmar que la privacidad no es importante (no tiene valor intrínseco) para Google y que esa información privada de la que dispone no es un fin en sí mismo sino tan sólo un medio para conseguir otro objetivo que en este caso sería la ganancia económica o el mantenimiento en una posición dominante respecto a sus competidores. En cierto modo tendrían razón a la hora de hacer tal réplica. Pero habría que analizar en este punto una situación fundamental en el ciberespacio a este respecto.

La cuestión principal aquí es que en el ciberespacio, que ya se ha dicho informacional, para todo agente que participe en este entorno, la privacidad es finalmente un medio para alcanzar un fin. No es una situación que atañe sólo a Google sino al ciberespacio en general. Cuando se ha propuesto la idea de una "privacidad analógica" se ha dicho que ésta tiene entre sus características ser una privacidad descontextualizada del lugar donde se desarrolla. Con esto se quería expresar esta idea de que la privacidad no es en el ciberespacio una cuestión de fines sino una de medios.

Cuando un usuario hace uso de su privacidad en la red, su objetivo principal es que la información que hay detrás de ella no sea accesible para el resto de usuarios. Así, una persona dispone de contraseñas para entrar en determinadas zonas de la red, como puede ser su correo personal, su banco o su cuenta en una red social. La necesidad de claves para el acceso viene determinado por ese desplazamiento de los quehaceres antes reservados al espacio privado a un lugar ahora eminentemente público. Las empresas e instituciones han creado zonas privadas, lo que se conoce como *intranet*, donde sólo es posible el acceso si se forma parte del grupo social, la empresa o

institución. Esto se debe en cierta medida a que mientras antes era necesario el acceso físico y personal a un lugar, ahora se hace de forma remota desde un espacio público.

No se puede decir de Google que no tenga la privacidad como un valor que hay que respetar. El hecho de que gestione grandes cantidades de información de sus usuarios y que la utilice como medio par alcanzar un fin, aunque en su caso sea uno económico, no la sitúa en una posición diferente a la del resto de agentes del ciberespacio, pues como se ha dicho más arriba la privacidad es un medio para todos los actores de la red.

Es cierto que el hecho que toda la red funcione de un modo en concreto no significa que esa actuación sea buena, ética o razonable por el simple hecho de que sea la forma general de actuación. Pero también es cierto que si todos los actores que participan de la red entienden la privacidad como un medio, no puede juzgarse a Google de actuar del modo habitual. De hecho, en la medida en que entiende la privacidad como un fin en sí mismo, actúa de un modo que podría decirse, más respetuoso con el concepto tradicional de privacidad. Analizada atentamente, teniendo en cuenta su política de privacidad, Google actúa de tal modo que la privacidad de los usuarios es atendida y respetada dentro de los márgenes posibles que la propia arquitectura de la red permite.

Se podría considerar que la acción de vender información sobre el tráfico y el uso de la red de los usuarios-compradores a los usuarios-productores es una vulneración de la privacidad de los primeros. Pero hay que tener en cuenta que este hecho no es exclusivo de la red como tampoco es novedoso de las tecnologías digitales. Este tipo de acciones, en las que entrarían los llamados estudios de mercado, son una práctica habitual de las ciencias de la sociología o la mercadotecnia. Cuando se realizan estadísticas sobre el comportamiento de una sociedad o un grupo de personas, como puede ser el número de vehículos que han circulado por una carretera en un tiempo concreto o cuando se informa de cuántas personas han participado en una manifestación, se está realizando la misma acción que hace Google cuando analiza el tráfico de Internet, es decir, analizar el comportamiento de las personas en un momento dado.

Se podría afirmar que la Dirección General de Tráfico (DGT) o las estadísticas del Instituto Nacional de Estadística (INE) sobre el consumo de los y las españoles es un servicio público que no pretender generar beneficios con esos datos y que la información de la que disponen no es tan

concreta como la que puede utilizar Google como el número de teléfono, el modelo de dispositivo, el tiempo de estancia en una web determinada, etc.

En esta comparación se pueden advertir varias cosas. En primer lugar, es cierto que las instituciones antes mencionadas son un servicio público y que no pretenden generar beneficios y por lo tanto el rastreo de información no pretende sino poner de manifiesto determinadas acciones ciudadanas. Además, se podría decir que el uso de radares para controlar el volumen de tráfico en una carretera no significa que cada coche, y su conductor, pueda ser identificado. Es cierto que el evitar retenciones o accidentes de tráfico, así como conocer las tendencias sociológicas de un grupo de población concreto pueden interpretarse como acciones que no están encaminadas a la obtención de beneficios y que por lo tanto se alejan de las intenciones de Google cuando recoge información sobre el tráfico de sus usuarios. Pero también puede decirse que en la medida en que el control de tráfico y los datos sociodemográficos ayudan a la gestión de una sociedad concreta están, en cierta manera, generando beneficios para esa sociedad.

La diferencia fundamental entre las actuaciones de estas instituciones y las de Google radica en que mientras unas están al servicio de los ciudadanos y los datos obtenidos ser gestionan para beneficiar a la población, la otra utiliza esa información en beneficio propio. En el momento en que estas instituciones comenzasen a beneficiarse así mismas sobre la información de la que disponen, se situarían automáticamente del lado de Google, dejarían de ser instituciones u organizaciones para convertirse en empresas. Es precisamente la diferencia entre ente público y privado lo que, para el ciudadano, garantiza al menos psicológicamente, la protección de los datos privados y la privacidad.

La cuestión en el ciberespacio radica en que una empresa privada gestiona la información personal de los usuarios. Pero hay que tener en cuenta que el lado opuesto sería que una empresa pública, esto es, el gobierno, controlase la información privada de los usuarios de Internet, situación que ya sucede en algunos países y que tiene como resultado la crítica por parte de organizaciones como Amnistía Internacional, Human Right Watch RSF, etc., por violar determinados derechos humanos.

Puede resultar preocupante que Google disponga y venda información referida al dispositivo móvil, el número de teléfono u otro tipo de información relacionada con el medio y modo de conexión a Internet. Pero este tipo de información no debiera ser considerada de tipo personal o privada. Del

mismo modo que la DGT puede saber cuántos Seat Ibiza han pasado por la M30 en un determinado momento del día o el INE conocer cuántas personas han preferido alojarse en un camping en vez de en un albergue o casa rural en el mes de julio de 2016, Google dispone de información relativa a su actividad, como las páginas visitadas, el tiempo de permanencia en ellas u otros datos relacionados con el tráfico en Internet.

Sería extraño pensar que la DGT o el INE están vulnerando la privacidad de los ciudadanos porque hagan estadísticas con los datos obtenidos de ellos. Esto se debe a que, como se ha dicho, son organismos públicos. Como Google se pretende un servicio gratuito, se tiende a pensar en ella como en una institución pública a la cual se puede cuestionar por el uso que haga de los datos personales de los usuarios. Pero lo cierto es que Google es una empresa privada y en cuanto el usuario acepta las condiciones de uso de los servicios que la empresa ofrece ésta puede hacer, dentro del marco de la legalidad, lo que considere más oportuno con los datos de los que dispone.

Otra cuestión diferente sería considerar si el marco legal en el cual se desarrollan las actividades en Internet es el adecuado para mantener la privacidad, tal y como se entiende actualmente. Pero esta es una cuestión que escapa a las competencias y posibilidades de esta investigación. Tan sólo señalar que sería posible una investigación completa sobre las leyes que rigen el ciberespacio, la adecuación de las leyes existentes en este espacio, ya no nuevo sino joven, y las posibles futuras normas que pudieran servir para acallar las preocupaciones de los ciberciudadanos en esta llamada aldea global.

5.6. Privacidad como control de la información en Google

El control sobre la información constituye una buena garantía para mantener la privacidad en el ciberespacio, por ello gran parte de la ciberética trata el tema de la privacidad partiendo de la idea que ésta debe basarse en el control sobre la información. De hecho, el problema fundamental de la privacidad en Internet radica en que el usuario no dispone de suficientes, o claramente definidas, herramientas de control sobre la gestión y el uso de la información que genera su estancia en el ciberespacio. La ciberética se preocupa, principalmente, por encontrar mecanismos donde los usuarios tengan más capacidad de decisión a la hora de controlar esa información. Para ello, apunta, es fundamental una serie de reglas o normas que rijan la gestión de esa información.

Sin embargo, recalcando la idea de un ciberespacio eminentemente público, un espacio digital donde la reproducción, almacenamiento y difusión es casi ilimitado, es difícil encontrar un modelo que permita el control total sobre la información generada. Una vez en el ciberespacio, la información adquiere, como afirma James H. Moor un carácter *grasiento* que dificulta su control, ya que se multiplica de tal forma que es casi imposible mantenerla en un lugar acotado y por ende controlado. "When information is computerized, it is greased to slide easily and quickly to many ports of call [...] Greased information is information that moves like lightning and is hard to hold onto" (Moor, 1997, p. 27). A pesar de este carácter deslizante, el control sobre la información resulta el modo más adecuado para mantener cierta privacidad en el ciberespacio. El problema estriba en conseguir frenar o minimizar la *grasificación* de la información, que en el medio en el que se desarrolla resulta realmente complicado, debido al carácter estructural de la red.

Prosiguiendo en el intento de una definición de privacidad que pase por el control sobre la información, es importante aclarar qué tipo de información debe ser considerada como privada y, por lo tanto, sujeta a control. Puesto que parte de la información que tradicionalmente se ha considerado privada ha dejado de serlo y no por una falta o abuso sino por las propias decisiones y actuaciones de las personas que han alejado de la privacidad determinada información y la han puesto al alcance del público.

La creación de un perfil en una red social, por ejemplo, pasa necesariamente por ceder el control sobre la información ofrecida a la empresa que gestiona esa red social. Así mismo, determinadas acciones como la posibilidad de compartir comentarios, imágenes y otro tipo de datos supone la cesión del control sobre información personal que se ha dado. Si un usuario utiliza una red social para anunciar que ha visitado una página web o que se ha comprado determinado producto, está compartiendo esa información en la red. Esto significa que está cediendo el control de esa información, no que lo está perdiendo. Al ceder ese control, Google podría utilizar esos datos en su propio beneficio sin que el usuario pudiera hacer nada al respecto. Sin embargo, cuando Google utiliza los datos de navegación, que vendrían a obtener los mismos datos que el usuario está haciendo públicos en las redes sociales, se tiende a considerar que está habiendo una pérdida de privacidad, lo cual resulta paradójico. De ahí la necesidad de definir y demarcar qué se entiende por datos personales o cuándo deben estar sujetos al control sobre su uso, de otro modo se darán situaciones en las que se vulnere y no se vulnere la privacidad al mismo tiempo.

Como se ha aclarado en su momento, la idea de la privacidad como control sobre la información es en cierto modo vaga e imprecisa. Se ha visto, con el ejemplo relativo a los datos de pacientes y el paso de información médica de unos sanitarios a otros, que la falta de control sobre la información no significa necesariamente la pérdida de privacidad, del mismo modo que el simple control sobre la misma no asegura una situación privada. Por eso algunas voces habían propuesto completar la idea de una privacidad basada en el control de la información pero entendida esta como control sobre el acceso a la misma. La privacidad en este sentido vendría asegurada por un acceso restringido a la información.

Las propuestas de Ruth Gavison y Anita Allen, recuérdese, iban encaminadas en este sentido. Para Gavison hablar de privacidad como simple control sobre la información resultaba insuficiente para asegurarla ya que, como se ha visto, podían darse situaciones donde el control sobre la misma no supusiera efectivamente un aumento de la privacidad. Proponía entonces entender la privacidad partiendo de la accesibilidad o inaccesibilidad a la información. Juzgaba también que el único modo de asegurar la privacidad de una persona o personas se podía conseguir por tres medios: el secretismo, el anonimato y la soledad. Anita Allen, por su parte, distinguía dos tipos de privacidad o ámbitos donde actúa. El primero era el relacionado con la información personal referida a los datos de la vida privada de las personas. El segundo estaba relacionado con la separación entre los espacios público y privado. En este sentido la privacidad significaba la no intervención exterior en la vida privada de las personas.

El punto de partida de ambas autoras, entender la privacidad como acceso restringido a la información, es un planteamiento acertado a la hora de entender la privacidad en el ciberespacio. De hecho, el acceso restringido es el modo en que los cibernautas ejercen su privacidad en este medio. Y como se verá más adelante, es precisamente ese acceso restringido el modo en que Google protege la privacidad de sus usuarios. Pero antes de verlo es necesario plantear algunas cuestiones sobre las propuestas de ambas autoras. El primer escollo que se puede encontrar a la hora de aceptar el supuesto que la privacidad sólo se puede conseguir por medio del secretismo, el anonimato y la soledad estriba en que estos conceptos parecen totalmente ajenos al sentido de ser del ciberespacio y resulta complicado ver cómo podría entenderse una privacidad digital atendiendo a estas características o modos de conseguirla.

Estos tres modos de privacidad llevan consigo, cada uno de ellos, unos conceptos que chocan con la idea y el modelo del ciberespacio en sí. El secretismo está determinado por el *acceso* a información. El anonimato, por su parte, tiene que ver con la *atención* puesto en una persona o grupo de personas. La soledad está estrechamente relacionada con la *proximidad* entre individuos. De entre estas tres características, tal vez la soledad sea la única que pueda conseguirse de un modo sustancialmente notable en el ciberespacio. En la medida en que casi cualquier acción de la vida cotidiana puede ahora realizarse de modo remoto, sin necesidad de entrar en contacto de forma directa con ningún individuo, la idea de una vida solitaria sin contacto humano presencial resulta plausible en el medio digital. Aunque esa soledad, esa distancia física con otros individuos no significaría por sí misma una privacidad total. Haría falta la desconexión con el ciberespacio para alcanzar esa privacidad. Pero lo que aquí se pretende es definir un tipo de ciberprivacidad, por lo que una soledad total basada en una desconexión absoluta con el ciberespacio alejaría el discurso de los objetivos de esta investigación. De este modo, la soledad debe ser desestimada para una definición de privacidad digital.

En cuanto al acceso a la información y la atención derivadas de los conceptos de secretismo y anonimato respectivamente, sucede que ambos aspectos son parte esencial del ciberespacio. Por un lado, si el acceso a información es parte fundamental de este espacio, debe serlo también en el concepto de privacidad que se quiera definir para este medio. Por otro lado, el concepto de secretismo que plantea Gavison, del que deriva la idea de acceso, puede llevar al ciberespacio más problemas que soluciones para la privacidad.

Podría suceder que se aceptase el secretismo en el ciberespacio como un buen método para salvaguardar la privacidad de los usuarios y que se empezara a utilizar como norma. Ciertamente sería de ayuda para mantener la información alejada de posibles abusos y los usuarios accederían así al control y acceso restringido de su información. Pero, hay que tener en cuenta que si el secretismo formara parte esencial de la forma de actual en el ciberespacio podría suceder que las empresas que lo gestionan hicieran del secretismo también su modo de actuar. Así, no sólo los usuarios no sabrían cómo se gestiona su información sino que, en un medio esencialmente informativo, la información estaría restringida para todos los agentes que componen el ciberespacio. Una situación que resultaría sin sentido ya que podría no haber acceso a ningún tipo de información. Por otro lado, parte de la preocupación sobre el uso de la información de los usuarios estriba en ese secretismo u ocultación sobre el modo de gestión de la información. Así pues, el

movimiento realizado para salvaguardar la privacidad significaría precisamente la pérdida de control sobre el acceso a la información y por tanto de privacidad misma.

Por último, la atención y el anonimato como formas de privacidad podrían ser un buen método para el ciberespacio. De hecho, estrictamente hablando, Internet ya es un lugar anónimo. La mayoría de los cibernautas navega por una red superficial, visible y pública para la mayoría de usuarios y empresas. Pero existe una red, llamada web profunda, que tiene como fundamento la idea de una navegación anónima. Su funcionamiento se basa en que los motores de búsqueda, como Google, no pueden indexar los sitios web contenidos en la web profunda. El navegador TOR (The Onion Router) permite a sus usuarios navegar de forma anónima, de modo que no su estancia en el ciberespacio no genere tráfico descifrable.

> Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going[72].

De modo que el anonimato en la red es la mejor forma de mantener la privacidad en el ciberespacio. La cuestión radica en que muchas de las acciones que el usuario común de Internet realiza en el ciberespacio no pueden llevarse a cabo en esta web profunda, de ahí que hayan permanecido separadas como dos redes diferentes. Atendiendo al ejemplo escogido en esta investigación, Google, no es posible mantener un anonimato como el ofrecido en la web profunda y seguir utilizando los servicios de la empresa escogida como ejemplo.

En el caso de Anita Allen, ella misma plantea la dificultad de entender la privacidad como acceso restringido. Su principal problema, como apunta, es que este acceso restringido puede llevar a la protección o desprotección de la privacidad al mismo tiempo. En el caso de los datos personales parece evidente que el control como acceso restringido es una buena forma de mantener la privacidad de las personas ya que éstas pueden gestionar y controlar su información. Aunque, de

---

[72] https://www.torproject.org/about/overview.html.en

nuevo, sería necesario definir qué se entiende por datos personales e información confidencial en el ciberespacio. La pregunta estriba en saber si toda la información generada en este espacio debe tenerse como información personal o si por el contrario existen algunos datos que no merecen tal atención, en la medida en que aun siendo información personal, en tanto relativa a una persona, su conocimiento público no suponga ningún obstáculo para la libertad y privacidad individual. En cualquier caso deberían ser los ciberciudadanos y por ende la ciberética, y no las empresas, quienes dicten qué datos deben ser tratados como personales y por lo tanto objeto de privacidad y cuáles pueden ser considerados como públicos o no sujetos a protección.

Por otro lado, los problemas que pueden derivarse de la privacidad como acceso restringido cuando se trata en espacios públicos o privados pueden darse también en el ciberespacio. La no intromisión en espacios privados en la red puede tener como resultado consecuencias inesperadas e indeseables. Ya se ha hecho referencia en algún momento de esta investigación (página 103) a situaciones de redes de pedofilia, al comercio de personas o a situaciones de ciberacoso. Actuaciones que de no ser por la vigilancia y el rastreo de la red, que desde el punto de vista del acceso restringido se estaría vulnerando la privacidad de los usuarios, se mantendrían sin ningún castigo. Alegando motivos de privacidad se estarían violando otro tipo de derechos fundamentales de los ciberciudadanos. Hay que tener cautela y mesura, como afirma Allen, a la hora de defender la privacidad ya que ésta llevada al extremo puede desencadenar situaciones de vulnerabilidad y desprotección social.

Dicho esto parece ser que la privacidad como acceso restringido no es suficiente, al menos en el sentido planteado por las autoras arriba citadas, para asegurar y mantener una privacidad real y factible de la información de los ciberciudadanos. Si bien es cierto que es la mejor y la más extendida en uso dentro de la red no deja de resultar insuficiente como definición apropiada para una privacidad que ante todo se desarrolla en un espacio abierto y accesible para todos. Tal vez el modelo más apropiado para una privacidad total en la red sea el modelo de la antes mencionada web profunda pero, un modelo basado en el anonimato en la red. En este caso, Google no tendría oportunidad de generar beneficios, la privacidad de los usuarios se mantendría pero dejaría de proveer de herramientas y servicios gratuitos.

La privacidad entendida como acceso restringido tiene como característica principal en el ciberespacio ser el modo más extendido y común en la red por un lado, al menos en la red

superficial[73], y por otro, la forma por la cual el usuario es capaz de tener cierto control sobre la información que genera en él. Se dice cierto control y no control total porque como se intenta demostrar en esta investigación resulta imposible tener un acceso completo a la gestión de la información dejada en el ciberespacio. El hecho que navegar por la red sea una acción fácil y más o menos instantánea para el usuario no significa que el funcionamiento y los elementos involucrados lo sean. Una simple conexión a Internet, con independencia de las búsquedas que se realicen, esto es, la conectividad misma, necesita una cantidad notable de agentes y herramientas que la permitan. Las empresas encargadas de las antenas, cables y satélites, los organismos y gobiernos involucrados en la gestión, financiación, control y supervisión de los mismos, los productores de los dispositivos, las empresas proveedoras de servicios, las compañías proveedoras de alojamiento en Internet, los motores de búsqueda, etc.

Todos estos actores forman parte de Internet y, en mayor o menor medida, disponen de información de los usuarios. Las antenas, cables y satélites reciben información sobre cada dispositivo que se conecta a ellos; los productores de dispositivos tienen conocimiento sobre qué usuario está haciendo uso de sus aparatos; las empresas proveedoras de servicios como pueden ser Orange, Vodafone o Movistar disponen de toda la información personal relativa a cada cliente; los motores de búsqueda tienen acceso a los datos de navegación de sus usuarios, etc. Sin embargo, las preocupaciones de los teóricos de la ciberética y los críticos con las tecnologías digitales no contemplan todos estos actores como posibles sujetos que deban preocupar a la privacidad de los usuarios y centran sus esfuerzos en realizar críticas y poner de manifiesto el control de determinadas empresas sobre la información relativa a los usuarios de Internet. Sin duda, estas empresas por separado no disponen de la información y el monopolio que sustenta Google y por lo tanto no son miradas con la misma precaución que el gigante de Internet.

Es evidente que Google, debido al volumen de información del que dispone, supone una fuente de preocupaciones para la ciberética, para los usuarios en general e incluso para las empresas competidoras en su sector. También es evidente que, debido a su poder dentro de la red, puede hacer un uso inadecuado de esa información. Ahora bien, hay que remarcar, como ya se ha hecho varias veces a lo largo de esta investigación, que toda la información de la que dispone es información que el usuario ha consentido que se recabe. Sin duda consentimiento no es aceptación sino tolerancia, incluso hacia una situación que puede considerarse de vulnerabilidad de derechos.

Aceptar las condiciones de uso de los servicios de Google significa estar de acuerdo con la gestión por parte de la empresa de la información que pueda gestionar mientras se hace uso del servicio. Se podría rebatir contra esto, como se ha señalado más arriba, que aceptar las condiciones de uso no significa estar de acuerdo con la forma de gestión de la información y que simplemente se está permitiendo que se haga uso de la información a pesar de no estar de acuerdo. Y sin duda así podría suceder. Pero hay que recordar que nadie obliga al usuario a aceptar esas condiciones.
El traspaso de información entre médicos y especialistas sanitarios a la hora de tratar a un paciente, el cotejo de datos entre entidades financieras, la solicitud por parte de determinados ministerios a otros de información personal de los individuos, como puede ser la presentación del certificado de antecedentes penales, etc., son movimientos de información personal que los individuos o ciudadanos no están en disposición de controlar. Es posible decidir ir o no ir a un especialista médico, no pedir un crédito o no presentarse a una oposición pública, situaciones éstas en las que se exige el acceso a este tipo de información. Pero las personas desean que su médico de cabecera reciba las pruebas enviadas al hematólogo, necesitan acceso a dinero que no disponen en ese momento y pretenden optar y lograr un puesto de trabajo en la administración pública. En este sentido están obligados a aceptar las "condiciones de uso" de esas situaciones.

Pero no sucede lo mismo en el caso de Google. Nadie está obligado a utilizar el navegador Google Chrome, abrirse una cuenta de Gmail, utilizar el GoogleMaps para ubicarse en una zona geográfica ni ver un vídeo de YouTube. Claro que la no obligación no significa que la privacidad de los usuarios deba ser desatendida, pero sí que limita o al menos pone en cuestión la exclusiva responsabilidad de Google por el uso de datos. Esta es una cuestión fundamental a la hora de tratar la privacidad de los usuarios ya que éstos desean acceder a todos los servicios que le permitan una navegación sencilla, cómodo, rápida y eficaz, lo que implica necesariamente (necesaria en el sentido de técnicamente necesaria actualmente, al menos en la web superficial) el uso de datos de personales.

El problema, desde el punto de vista aquí expuesto, es la definición misma de datos personales. Pues ésta implica una serie de conceptos y datos que no dan cabida a una funcionalidad del ciberespacio sin que de un modo u otro se atente contra la privacidad de los cibernautas. Es necesaria una revisión del término de modo que se pueda asegurar una navegabilidad por la red, que permita la utilización de los servicios al tiempo que se proteja la privacidad de los individuos. Sin

esta nueva contextualización hacer uso de los servicios de Internet siempre conllevará una pérdida parcial o total de la privacidad, al menos en la forma actual del ciberespacio y su seguridad. Es necesario destacar, así mismo, que se dan situaciones en las que el usuario no es informado o al menos no de una forma suficientemente clara sobre cómo se están utilizando sus datos y para qué. La aceptación de las condiciones de uso, del mismo modo que los consentimientos informados médicos, no tienen en cuenta el grado de comprensión de los individuos a la hora de firmar el acuerdo.

Toda la Política de privacidad de Google tiene como objetivo informar al usuario sobre los datos que se recogen a la hora de utilizar sus servicios, el uso que se dará a los mismos y las formas que tiene el usuario de acceder a esos datos. Muchos de los servicios que la empresa ofrece necesitan el registro del usuario, creando así una cuenta Google. Este método implica que deberá ofrecer a Google datos personales. Con estos datos se pretende ofrecer un servicio personalizado y una experiencia única para cada usuario, así como publicidad basada en su comportamiento, al menos esa es la intención alegada por la empresa. Por otra parte, permite que solamente el usuario en cuestión sea capaz de acceder a determinados servicios. Al crear una cuenta de Gmail, el cibernauta que desee abrir la cuenta, deberá incluir datos como el número de teléfono, la fecha de nacimiento, una clave de acceso, así como responder a unas preguntas de carácter personal que serán utilizadas en el caso de olvidar la contraseña de acceso o ante el bloqueo de la misma por la tentativa de terceros de acceder a la cuenta.

Estos datos, entre los que se incluyen la fecha de nacimiento, el número de teléfono, preguntas de seguridad del tipo el nombre de soltera de la madre, el nombre de la primera mascota, del primer colegio, etc., son considerados como información de tipo personal y puede suponerse que el acceso por parte de Google a esa información sobrepasa los límites de la privacidad de los individuos y de hecho, efectivamente es información personal en la medida en que es relativa a la persona y sólo a una persona. Ahora bien, cabe preguntarse si este tipo de información debe ser protegida como información personal privada, esto es, defendible bajo el paraguas de la privacidad.

Antes del surgimiento de las tecnologías digitales cualquier persona podía acceder al número de teléfono de otra. Las Páginas Blancas, como las Páginas Amarillas, eran distribuidas de manera gratuita y anual por la compañía de teléfonos Telefónica en todas las casas de España. Cuando una persona quería buscar los datos de contacto de una empresa lo hacía en las Páginas Amarillas, del mismo modo que se hacía para localizar el teléfono de un particular en las Páginas Blancas. En

ningún momento se consideraba que esa aparición en las Páginas Blancas suponía una pérdida de privacidad para el usuario, tan sólo era considerado el medio normal y natural de poder contactar con alguien y/o de ser contactado. Es a raíz del surgimiento de las tecnologías digitales y en concreto del auge y generalización del uso de telefonía móvil que se ha empezado a considerar el número de teléfono como un dato personal que hay que proteger con privacidad.

Un camino parecido han seguido determinados datos como el nombre de soltera de la madre o de soltero del padre, el nombre de la primera mascota o del primer colegio. Todas estas preguntas que ahora se utilizan como preguntas de seguridad para acceder a servicios, no han sido consideradas como preguntas privadas hasta el momento en que las respuestas a las mismas, junto con otro tipo de información, pueden ser utilizadas para acceder a espacios particulares de cada cibernauta. Conocer el nombre de la madre o del padre del vecino no suponía tener acceso a su información personal. De hecho podría decirse que resultaba irrelevante. Su conocimiento o ignorancia no suponía más que el conocimiento de un dato en concreto de la vida de otra persona, sin más trascendencia que saber que esa persona vivía en el piso segundo o en el entresuelo o que iba a comprar el pan a la panadería de la misma calle donde vivía o que recorría dos kilómetros para hacerse con una barra de pan.

Es el momento en que la información se transforma en mercancía, con las tecnologías digitales y el uso normalizado y estandarizado de las mismas, cuando la información se convierte en un bien de consumo, cuando toda información, con independencia de su origen o procedencia, se transforma en un objeto que hay que proteger y por lo tanto objeto de la privacidad.

El acceso restringido a la información como modelo para proteger la privacidad de los usuarios puede entrañar, como afirma Anita Allen, situaciones que devengan problemáticos a la hora de proteger la privacidad. Hay que tener en cuenta que Google actúa de modo que el acceso a la información sea siempre de un modo restringido, ya se sea creando mecanismos para que los usuarios tengan un mayor control sobre la información que generan al hacer uso de sus servicios o exigiendo la creación de cuentas personales con restricciones de entrada, de ahí los medios que pone al alcance de los usuarios para la gestión de su información o la exigencia de claves, contraseñas o preguntas de seguridad, la posibilidad de navegar en modo incógnito, deshabilitar las cookies, etc.

Existe otro medio por el cual Google protege la privacidad de sus usuarios partiendo de la idea del acceso restringido. Es un modo en el que, efectivamente, el acceso restringido a la información sucede. El problema es que es la propia empresa y según sus propios criterios, ya se han visto económicos y de posición dominante, quien da acceso o no a determinada información. Cuando se crea una cuenta Google, como por ejemplo para tener acceso al servicio de vídeos YouTube, el usuario y su información están protegidos con un acceso restringido, protección que brinda la empresa, recuérdese, en principio de forma gratuita.

Ahora bien, como gestora de esa información, Google puede decidir cuándo y a quién otorgar acceso a la misma. En principio la privacidad como acceso restringido se mantiene en este caso, no todo el mundo tiene la posibilidad de acceder a esos datos pues es una cuenta con acceso personal, el usuario puede gestionar esa información como le parezca, editándola, borrándola, etc., y Google ofrece las herramientas para llevar a cabo toda esa privacidad.

Sin embargo, y como se ha dicho en repetidas ocasiones en esta investigación, Google trabaja con dos tipos de usuarios, los consumidores y los productores. Con ellos mantiene diferentes relaciones clientelares, es decir, a unos y otros les ofrece diferentes servicios. Mientras a unos les ofrece servicios, entre otras cosas, para la edición, subida o visualización de vídeos de forma gratuita, a otros les ofrece la posibilidad de acceder a determinada información para que puedan vender sus productos a determinado segmento de población. Es un acceso limitado, puesto que Google ofrece a los usuarios-productores fragmentos de información, la suficiente o necesaria para que éstos tengan capacidad de centrar sus esfuerzos en un público objetivo concreto. No se trata de abrir las puertas de la cuenta personal del usuario-consumidor, la información personal de éste se mantiene en forma de acceso restringido, pero es Google quien dicta las restricciones de este acceso.

En este sentido la privacidad como acceso restringido se está respetando, el usuario-consumidor tiene sus datos personales de su cuenta de YouTube protegidos de posibles intrusiones de terceros. Pero al mismo tiempo se da la situación de que determinados fragmentos de esa información son expuestos a otros usuarios, en este caso los productores. Este hecho no conlleva la pérdida de la primera situación, pues el acceso restringido se mantiene pero es Google quién determina las posibilidades de ese acceso. Este es el mayor problema de entender la privacidad como acceso restringido desde la perspectiva usuario-Google, existe la posibilidad de aun teniendo este tipo de control sobre la información ésta pueda verse desvelada de algún modo. Por otra parte, desde el

momento en que se firman las condiciones de uso de los servicios de Google, donde se le ceden los derechos de uso de la información, la compañía puede permitir el acceso a ésta a quien quiera y cuando quiera, en calidad de dueña de esos datos.

Esto sucede principalmente porque, como se ha dicho, Google trabaja con dos tipos de clientes. Su Política de privacidad no los diferencia de un modo explícito. Por lo tanto, cuando se refiere a temas como la protección, la seguridad o el beneficio de sus usuarios resulta complicado entender a cuál de ambos usuarios está haciendo referencia. Este hecho que podría resultar trivial no lo es en absoluto ya que la protección, seguridad o beneficio de unos va en detrimento de la protección, seguridad o beneficio de los otros. Si se protege la privacidad de los usuarios-consumidores se está dejando a los usuarios-productores sin modo de desarrollar sus negocios, que por otra parte son demandados por los consumidores. Si se asegura la capacidad de actuar de los productores se están vulnerando los derechos de privacidad de los consumidores. En consecuencia, el beneficio de unos es la pérdida de los otros.

En este sentido la Política de privacidad de Google resulta insuficiente para la protección de la privacidad de los usuarios-consumidores pero netamente beneficiosa para los usuarios-productores y para Google misma. Estos últimos usuarios están protegidos con los mismos mecanismos esgrimidos en la Política de privacidad que tienen los usuarios-consumidores, sin embargo, éstos padecen la desprotección o la vulneración de la misma al ejercer la misma política para ambos grupos.

Si Google quisiera tener una actuación equitativa entre ambos usuarios debería, por un lado, separar ambos grupos explícitamente de modo que cada uno tenga sus derechos y obligaciones en el uso de los servicios que ofrece la empresa. Por otra parte, debería redactar dos tipos de políticas de privacidad y de condiciones de uso, donde cada grupo de usuarios pudiera saber en todo momento qué se está haciendo con sus datos, cómo se están gestionando y los resultados que la gestión de esa información está suponiendo para la privacidad de todos ellos. Mientras no se consigan estos pasos, Google podrá ser objeto de crítica por parte de la ciberética en cuanto a gestión de la privacidad se refiere y los usuarios podrán seguir temiendo que sus datos sean utilizados de un modo que no se ajuste a la realidad que se les expone.

Hay que tener en cuenta, sin embargo, que como empresa privada, Google puede permanecer en su modo de actuar tanto como le permita la ley. Sin la intervención pública que imponga un determinado modo de gestión de la información en el ciberespacio, sin una conciencia social que imponga a las empresas, y a sí misma, actuar de un modo, llámese razonable, éstas y las instituciones privadas involucradas en aquél no tienen más obligación que la de cumplir las pocas normas que actualmente rigen este espacio. Más allá de éstas lo que cada empresa haga con sus condiciones de uso, sus políticas de privacidad y su gestión de datos personales es una decisión estratégica y empresarial con ninguna imposición moral o ética en sus prácticas.

Esta reflexión puede resultar poco edificante en términos éticos y se podría argumentar que aunque no haya presiones externas a las empresas privadas éstas deberían actuar de un modo moralmente bueno para la sociedad lo que en Google se traduciría por respetar la privacidad de las personas usuarias de sus servicios. Pero este es un argumento alejado de la realidad empresarial y económica actual, donde prima más el beneficio que la causa social. A pesar de ello una reflexión a este respecto puede servir de apoyo para ver cómo la conciencia social se está abriendo camino en determinados sectores económicos. Conciencia y responsabilidad que puede esperarse en el futuro para las empresas que operan y gestionan Internet.

Cierto es que todas las empresas podrían actuar de modo que las consecuencias de sus actos fueran en beneficio de la humanidad. Que GlaxoSmithKline dirija sus esfuerzos en desarrollar una vacuna contra la malaria o que la entidad financiera Triodos Bank utilice el dinero de sus clientes para la realización de acciones con fines sociales son efectivamente actuaciones de este tipo. Pero no dejan de ser decisiones empresariales y privadas. La responsabilidad social corporativa que llevan a cabo muchas empresas responde a este interés de actuar de un modo beneficioso para la sociedad, con independencia del mercado de actuación de las empresas. Ejemplos con la Obra Social de LaCaixa, las becas BBVA, los proyectos llevados por Iberdrola contra el cambio climático siguen esta línea de actuación. Si bien muchas de las acciones pueden verse como estrategias empresariales, lo cierto es que, con independencia de los motivos principales, son propuestas que se están efectuando.

El ciberespacio no es ajeno a esta responsabilidad social corporativa, como tampoco lo es Google. Según la revista Forbes, en mayo de 2016 Google era considerada la segunda mejor empresa para trabajar en el mundo[74]. Se sabe que sus instalaciones disponen de todas las facilidades para sus

[74] http://www.forbes.com/companies/google/

trabajadores y familia y que éstos tienen cierta capacidad de decisión en los futuros proyectos. También dispone de un amplio sistema de becas y ayudas a estudiantes. Puede decirse que la empresa es apreciada por su fuerte responsabilidad social corporativa.

Ahora bien, su causa pendiente, el apoyo total a la privacidad de sus usuarios, el apoyo a un Internet anónimo y privado choca frontalmente con su modelo de negocio. Por lo tanto, si se pretende que Google respete de un modo exigente la privacidad en el ciberespacio esto debe pasar necesariamente por una legislación más fuerte y tajante al respecto. Situación que podría desembocar en una modificación sustancial del uso gratuito de los servicios que ofrece la empresa e incluso de la pérdida total de los mismos. Los usuarios, la comunidad de Internet y todos los agentes involucrados en el ciberespacio deberán valorar las consecuencias de una posible legislación al respecto.

Para los usuarios de la red profunda y para los teóricos y analistas de la ciberética esta decisión es fácil de tomar y cualquier acción encaminada a la preservación de la privacidad en Internet será bien recibida. Pero hay que tener en cuenta también la opinión y el modo de uso de esa otra Internet, la red que es utilizada por millones de usuarios que quieren estar conectados a sus redes sociales, que quieren comprar de un modo fácil y rápido, que se les muestre la información que buscan y que pueden no querer una red más segura para sus datos sino mantener los mismo servicios que ahora se les ofrece.

Esto remitiría al tercer aspecto que se ha señalado como característico al hablar de la privacidad analógica, esto es, un concepto de privacidad que puede no ser compartido por todos los miembros de la comunidad del ciberespacio. Las redes sociales en todas sus variantes, ya sean de amistades, de imágenes, de comentarios, laborales, etc., los blogs, los comentarios u opiniones que pueden dejarse en cualquier página web, etc., evidencian una tendencia hacia el exhibicionismo en la red. Los cibernautas quieren darse a conocer en el ciberespacio, mostrar su vida en imágenes, sus ideas y pensamientos en comentarios, su conformidad o desacuerdo con determinados, o todos los asuntos sociales. La privacidad en este sentido, ha dejado de entenderse como aquello oculto a la mirada pública, para convertirse en una herramienta (valor instrumental) destinada a la gestión de la vida personal en el espacio público. Es por lo tanto necesario pensar un nuevo modelo de privacidad, donde los ciberciudadanos puedan seguir disfrutando de este espacio social pero mantengan niveles de privacidad que les hagan sentirse seguros en él.

Así mismo, como se ha comentado en otro momento (páginas 111 y ss.), la personalización de las búsquedas, y del uso de Internet en general, no debería ignorarse si se pretende hacer de la red un espacio privado, pues esta maquetación de los contenidos no podría darse sin el uso de información personal para diseñar un Internet para cada cibernauta. Si bien es cierto que pueden darse situaciones como las propuestas por Pariser, donde los contenidos ajenos al modelo de usuario desaparezcan de la red, también es importante señalar que esa personalización puede suponer, para determinada población, cierta seguridad a la hora de navegar por el ciberespacio. Hay que tener presente que existen usuarios para los cuales la personalización es una buena herramienta para encontrar la información que buscan. El uso que puedan hacer de Internet no está encaminado a la adquisición de conocimiento, amplitud de miras y cotejo de nuevos argumentos sobre las opiniones propias. Para muchos cibernautas el ciberespacio es un espacio más de socialización, consumo y divertimento. En este sentido, la personalización de contenidos es una herramienta deseable para esos fines. Estos usuarios, que también forman parte de la comunidad de Internet, tal vez no deseen una red más privada sino una que les permita seguir compartiendo y haciendo un uso social de la misma..

Internet, la ciberética y por ende la privacidad en el ciberespacio han sido pensadas, creadas y modeladas por inmigrantes digitales. Esto tiene como consecuencia más directa que éstas han tenido que aprender a socializarse, esto es adaptarse, a un medio totalmente nuevo y desconocido. Sin duda la forma más sencilla o cuanto menos la primera reacción ante una situación de esta índole pasa por reproducir los modos de hacer, pensar y actuar conocidos, comprobando si éstos funcionan en el nuevo espacio. Tal vez, las generaciones actuales y futuras, los nativos digitales, que no han conocido el mundo analógico y las reglas que lo rigen, o regían, no entiendan ni compartan determinados puntos de vista y modos de actuar de esa sociedad para ellos desconocida, incluida la idea de una privacidad basada en la separación de las esferas pública y privada, cada una de ellas con un tipo de información concreta que no puede o no debe ser expuesta en una esfera que no le corresponda.

5.7. Privacidad como acceso restringido en Google y cookies

Una de las cuestiones que mayores problemas puede acarrear a la hora de hablar de privacidad como acceso restringido en Google tiene que ver con el uso de cookies. En su momento (página 133) las cookies se han definido como un conjunto de datos que las páginas web envían al navegador para que éste pueda almacenar determinada información para su posterior uso. Como la

definición dada decía, las cookies permiten al cibernauta disfrutar de una experiencia del usuario más satisfactoria que sin ellas.

Google en concreto dispone de seis tipos de cookies (al menos ese es el número que destaca en su Política de privacidad) que permiten el almacenamiento de información en el navegador del usuario. Cada una de ellas cumple una función determinada. El uso de cookies, como se verá más adelante, no significa automáticamente la vulneración de la privacidad de los usuarios. Muchas de ellas tienen una finalidad técnica, permitiendo el correcto funcionamiento de una web. Otras facilitan o posibilitan que el usuario pueda realizar determinadas acciones, como pueden ser las compras en línea, otras que pueda entrar en determinados espacios reservados a los subscriptores o usuarios registrados. Este tipo de cookies, a pesar de utilizar datos personales de los usuarios, no se consideran "peligrosas" para la privacidad, en la medida en que reportan algún tipo de funcionalidad (beneficio) para el usuario. Sin embargo, existe un tipo determinado de cookies que sí pueden considerarse conflictivas para la privacidad de los usuarios.

Entre las cookies destinadas a la funcionalidad están las cookies de preferencias. Éstas son aquellas cookies destinadas a editar de forma única el navegador y las búsquedas de cada usuario. Este tipo de galleta informática permite que el navegador recuerde preferencias como el idioma, la región en la que se conecta, el uso de filtros como el SafeSearch, el número de resultados que se desean ver en una página, etc. Las cookies de preferencias tienen como objetivo la experiencia del usuario.

Otro tipo de cookies que Google utiliza son las denominadas cookies de seguridad. Éstas son las utilizadas para autenticar al usuario. Estas cookies son utilizadas en todos los sitios web donde es necesaria la autenticación de un usuario. Redes sociales, bancos virtuales, tiendas online o el acceso a determinados espacios donde es necesaria una cuenta privada para su entrada contienen este tipo de cookies. Todas aquellas web con el protocolo "https" usan este tipo de cookies ya que el usuario deberá dar algún tipo de información personal, incluidas las contraseñas, para su acceso. En el caso de Google son las denominadas "SID" y "HSID" las que permiten la encriptación de ese contenido sensible para proteger los datos personales de sus usuarios.

Las cookies de procesos, también utilizadas por Google, permiten el funcionamiento de un sitio web, esto es, poder navegar de una página a otra. Para pasar de la página de inicio de la Wikipedia a un artículo concreto, por ejemplo, son necesarias este tipo de cookies, de modo que el usuario puede

avanzar y retroceder por el sitio web. En el caso de Google este tipo de galleta informática permite el acceso a determinados documentos e información. Así, por ejemplo, la cookie denominada “lbcs” permite que el servicio de GoogleDoc abra documentos en el navegador.

Google también utiliza cookies con finalidades publicitarias, para “hacer que la publicidad sea más atractiva para los usuarios y más valiosa para los editores y anunciantes”. Estas cookies permiten que el usuario reciba publicidad relevante, esto es, cercana a sus posibles intereses y evitar que se repitan anuncios ya vistos, lo que para los usuarios-productores significa poder sacar más rendimiento a sus campañas. Estas galletas informáticas se utilizan para recordar las búsquedas más recientes de los usuarios, su interacción con determinada publicidad mostrada en los resultados de búsqueda y el seguimiento de las visitas a los sitios web de las empresas anunciantes. Este tipo de cookies también se encuentran en determinados servicios de Google como YouTube, de modo que puedan mostrarse los anuncios más relevantes en función de las búsquedas de vídeos y poder hacer un seguimiento de la interacción del usuario con éstos.

Dentro de este tipo de cookies existe una denominada “__gads” ofrecida por DoubleClick que, aunque es propiedad de Google, no puede leerla y tampoco tener acceso a la información que recoge, ya que ésta se incluye dentro de dominios que no son de Google. Principalmente, su objetivo es medir el número de veces que un usuario interactúa con un anuncio en concreto que se encuentre en esa web, de modo que se pueda evitar que el usuario vea muchas veces un mismo anuncio.

Entre estas galletas informáticas de publicidad Google hace uso de las denominadas galletas de conversión, que permiten al anunciante y a Google saber cuántas veces se ha acabado comprando el producto que se ha anunciado. Así mismo ayudan a comprobar si un usuario ha realizado un clic en un anuncio concreto. Éstas son también utilizadas, junto con los datos de usuario, para vincular esa información entre los diversos dispositivos que un usuario pueda utilizar. Este tipo de cookies tienen una permanencia limitada. Los datos que se recogen con estas cookies son compartidos con los anunciantes de forma anónima de modo que éstos sólo tienen acceso al cómputo total de veces que se ha clicado o se ha realizado una venta sobre un producto, no sobre el usuario concreto que ha clicado sobre el anuncio o ha hecho una compra.

La cookies de sesión recaban información sobre la forma en que los usuarios navegan por la red en una sesión determinada. Este tipo de cookies no son permanentes, esto es, no se instalan en el navegador, sino que son temporales y se borran cuando se cierra el navegador o la sesión. Estas galletas informáticas no influyen en el funcionamiento de la web por lo que su deshabilitación no repercute en la navegación. En Google estas cookies permiten generar un historial de las páginas visitadas por un usuario durante el período que el navegador permanezca abierto. De este modo permiten al usuario recuperar o volver a páginas que haya visitado con anterioridad. YouTube, por ejemplo, utiliza estas cookies para realizar un historial de vídeos que se han visto desde un navegador determinado.

La forma más conocida y fácil de entender este tipo de cookies son los "carritos de compra" de las páginas web. Cuando se realiza una compra en línea y se deposita un producto en el carrito de la compra, son las cookies de procesos las que permiten que la web almacene esos productos mientras que el usuario continúa navegando por la web. Sin éstas, sin el mecanismo que almacena esa información, al avanzar o retroceder por un sitio web se perdería esa elección de productos.

Por último, Google utiliza unas cookies para su servicio de Analytics. Esta herramienta, como se ha mostrado con anterioridad, realiza un análisis estadístico sobre la interacción de los usuarios con las páginas web. Estas cookies permiten recoger información sobre la navegación de los usuarios, siempre de forma anónima, por la red. Así, permiten a un determinado sitio web, por ejemplo, saber cuántos usuarios han visitado la página, desde qué dispositivo, cuánto tiempo han permanecido en ella, cómo se han movido por el sitio, etc. Combinada con otras cookies publicitarias, éstas son utilizadas para mostrar anuncios relevantes para los usuarios.

A la vista de esta explicación y definición de las diferentes modalidades de cookies que Google utiliza, se puede decir que no todas repercuten negativamente en la privacidad de los usuarios, incluso algunas sirven para su protección. Muchas de ellas son tan sólo unos de los muchos mecanismos que permiten el correcto funcionamiento de la red. Las cookies de preferencias o de seguridad estarían dentro de esta categoría de cookies que permiten al usuario navegar por la red de un modo ágil y personal así como también seguro. Del mismo las cookies de procesos permiten el paso de una página web a otra sin que esto suponga un inconveniente a la privacidad.

Sin embargo, existen otro tipo de cookies de Google que pueden suponer una pérdida de privacidad o cuanto menos una puesta en cuestión de la seguridad de ésta. Estas cookies son las relacionadas con la publicidad y la gestión de la misma, donde entrarían las de publicidad propiamente dichas, las de estado de la sesión y las de Google Analytics. Hay que tener presente que en este momento sólo se están incluyendo las cookies relativas a la Política de privacidad de Google, pero no son ni mucho menos las únicas existentes, ni en Google ni en la red, y que también pueden suponer una vulneración de la privacidad. Entre éstas estarían, por ejemplo, las denominadas cookies de terceros.

Según la definición de la Agencia Española de Protección de Datos las cookies de terceros "son aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio que no es el gestionado por el editor, sino por otra entidad que trata los datos obtenidos a través de las cookies"[75]. Cuando se quiere compartir un artículo o cualquier otro documento de una web en concreto a una red social por ejemplo, y la web permite hacerlo desde su dominio, son este tipo de cookies las que permiten realizar esa acción. El problema de éstas ante la privacidad es que al aceptar la política de cookies de una página que utilice este tipo de galletas informáticas se está aceptando que otras empresas tengan acceso a datos de navegación del usuario. En este sentido se está perdiendo el control sobre el acceso a la información que se está generando en la red. Hay que tener en cuenta que aceptar las condiciones de uso de una web concreta no debería significar aceptar las condiciones de otra.

Volviendo a las cookies utilizadas por Google y que aparecen en su Política de privacidad, aquellas que pueden crear conflicto con la privacidad son las relacionadas con la gestión de la publicidad. Éstas tienen como función principal ofrecer información del usuario-comprador a los usuarios-productores, de modo que puedan llegar a un público objetivo. Este hecho, de entrada, pone en evidencia un aspecto complicado de resolver. Se ha dicho en repetidas ocasiones que Google ofrece servicios gratuitos para sus usuarios-compradores pero que éstos ofrecen a su vez, en forma de pago, datos e información con los que Google podrá obtener beneficios al vender esa información a los usuarios-productores.

---

75 https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

Esas cookies, que permiten a Google ofrecer a los usuarios-productores información sobre el público objetivo de sus campañas, el modelo de usuario en cada sitio web, el rendimiento de estos sitios, el acierto o no de las campañas publicitarias, vender espacios publicitarios, y todas aquellas acciones que tengan que ver con el uso de datos de los usuarios y la publicidad en Internet, son también aquéllas que más pueden vulnerar la privacidad de los cibernautas, ya que su objetivo principal es ofrecer información sobre el tráfico web y el consumo de los cibernautas. Pero, hay que tener en cuenta que a su vez son el medio por el cual Google obtiene beneficios. Por eso, será difícil encontrar políticas que protejan a los usuarios de este tipo de cookies y que Google mantenga el modelo de negocio donde los usuarios-consumidores dispongan de servicios gratuitos y las empresas puedan seguir gestionando sus negocios en línea.

Se podría afirmar que el uso de la ventaja informativa de la que dispone Google conlleva resultados que pueden tenerse como poco éticos, al menos desde dos puntos de vista relacionados, cada uno de ellos, con los dos modelo de usuario. Google no sólo dispone de la información de los usuarios en la red mediante el uso de sus servicios sino que también es la empresa encargada de casi la totalidad de la publicidad en línea y la supervisora del tráfico web. Como tal, podría decirse que ejerce un monopolio sobre todos los recursos y mecanismos que puede reportar algún beneficio económico en el ciberespacio.

Podría pensarse que Google no consigue beneficios cuando alguien realiza una compra en una tienda virtual puesto que la transacción se realiza entre el vendedor y el comprador. Pero hay que tener en cuenta diversos factores que han mediado en esa compra-venta y de los cuales Google forma parte. Entre estos se encuentran la aparición de ese vendedor en determinado sitio web, que propicia que el comprador lo conozca o tenga presente. Del mismo modo sucede si aparece como enlace patrocinado en los resultados de búsqueda del usuario. También influye la consulta de estadísticas web que han posibilitado una campaña publicitaria concreta hacia un público objetivo, etc. En todas estas acciones Google ha tenido su parte de intervención, ya sea mediante Google Analytics, a través de la venta de publicidad introducida junto a los resultados orgánicos de las búsquedas de sus usuarios o en espacios publicitarios de sitios web concretos, u ofreciendo información relativa al tráfico y comportamiento del usuario. En este sentido Google no sólo ha facilitado esa transacción sino que ha generado beneficios para sí misma mediante ésta.

En este sentido, proporcionando toda la estructura que permite el mercado en línea, Google ejerce un control sobre las empresas, esto es, sobre los usuarios-productores, que la coloca en una posición de monopolio y de competencia desleal en la medida en que las empresas no disponen de alternativas reales que les permitan desarrollar su actividad en el ciberespacio. En julio de 2016 la Comisión Europea investigaba a Google por incumplir la normativa europea de competencia empresarial y le acusaba de abuso de posición dominante en el mercado de la publicidad en línea. La comisaria Margrethe Vestager se refería a la empresa en estos términos:

> Google ha ofrecido muchos productos innovadores que han sido fundamentales en nuestras vidas, pero esto no le da el derecho a denegar a otras empresas la oportunidad de competir e innovar. Hoy hemos reafirmado nuestro argumento de que Google ha otorgado preferencia de forma indebida a su propio servicio de comparación de precios en sus páginas de búsqueda general de resultados, lo que significa que los consumidores podrían no ver los resultados más pertinentes en sus búsquedas. También nos suscita reservas el hecho de que Google haya obstaculizado la competencia al limitar la capacidad de sus competidores para mostrar anuncios de búsqueda en sitios web de terceros, lo que suprime el margen de elección de los consumidores y la innovación[76].

En cuanto a los usuarios-consumidores, el uso de cookies de publicidad conlleva algunas cuestiones relativas a la seguridad de su privacidad. Es cierto que las cookies de publicidad sirven para que el usuario pueda ver publicidad relacionada con sus intereses. Así mismo que al usuario no se le repitan los mismos anuncios indefinidamente en las páginas web que visita hace que la experiencia del usuario sea, en general, más agradable. Por último, y del mismo modo, los enlaces patrocinados relativos a las búsquedas realizadas así como su aparición de un modo no invasivo, esto es, en el mismo formato que los resultados de búsqueda, influye de una forma positiva en el modo de navegar por la red, sin tener que cerrar ventanas emergentes o verse distraído por anuncios que aparten la atención de la acción que se está llevando a cabo. Todos estos modos de publicidad, basados en el uso de cookies, permiten a Google generar beneficios sin que se vea comprometida la privacidad de los usuarios. Ahora bien, no sucede lo mismo con todos los mecanismos publicitarios que Google despliega. Sin entrar en detalle en cada una de las cookies publicitarias, se puede hacer un análisis que ponga de manifiesto esta capacidad de vulnerar la privacidad de los usuarios.

---

[76] Recuperado de http://europa.eu/rapid/press-release_IP-16-2532_es.htm.

Cuando se insertan cookies publicitarias en los navegadores de los usuarios no se consigue mejorar la experiencia del usuario más allá de que éste no veo muchas veces un anuncio concreto. Lo que se pretende es formar un perfil de consumidor que permita a Google vender espacios publicitarios a un precio competitivo para las empresas y beneficioso para ella misma.

Los datos de tráfico web no reportan al usuario ningún beneficio concreto e incrementan las posibilidades de vulneración de su privacidad, en la medida en que se está cediendo a terceros, esto es, a las empresas, información relativa a la hora de conexión, el modo de navegación, el modelo de dispositivo desde el que se está navegando, el tiempo de estancia en una web, etc. Si bien es cierto que estos datos no se recogen de forma individualizada, todos estos datos forman parte, actualmente, de lo que se consideran datos personales, y por lo tanto, sujetos a las normas de la privacidad. En este sentido, Google está vulnerando el derecho de los cibernautas.

Así mismo el uso de cookies de publicidad supone la pérdida de capacidad de control sobre el acceso a la información por varios motivos. El primero de ellos es que se inserta en el navegador del usuario una herramienta que permite recabar información sobre el comportamiento del usuario sin que éste sea capaz de a) gestionar dicha herramienta; b) controlar qué tipo de información se está recogiendo; y c) sin saber ni poder controlar a qué empresa(s) se está(n) cediendo/vendiendo esa información. En segundo lugar, al convertir la información personal del usuario en una mercancía ésta se vende a todo aquel que esté dispuesto a pagar el precio que marca la compañía. De este modo el usuario es alienado de su propia información. Como esta información se puede vender a diferentes compradores y para diversos fines la pérdida del control sobre esa información es casi total. Una vez vendidos esos datos pueden ser vendidos otra vez por el primer comprador a un segundo comprador y así indefinidamente, adquiriendo entonces la información ese carácter grasiento del que ya se ha hablado con anterioridad.

Sin duda la cuestión de las cookies está determinada por una forma concreta de entender la privacidad y los datos personales. Si fuera posible eliminar de ambos conceptos los datos relativos al uso que los usuarios hacen de la red y el modo en que navegan por el ciberespacio, el problema de las cookies se reduciría considerablemente. No sería necesario preguntarse sobre el uso de información relativa al tráfico web o al comportamiento del usuario en el ciberespacio. El problema que aun permanecería sobre el uso de las cookies sería la injerencia sobre los dispositivos de los usuarios. La introducción de archivos en los dispositivos de los usuarios podrían entenderse como

una intromisión en la privacidad de los usuarios, ya que se estaría manipulado o modificando elementos que no forman parte del ciberespacio y que no son de carácter público.

La cuestión de las cookies y la privacidad ha tenido como respuesta que los organismos internacionales se posicionen ante el uso de estas herramientas para almacenar información de los usuarios. La directiva del Parlamento Europeo de 2002 ratificaba una serie de acciones necesarias en materia de protección de datos de los consumidores en Internet[77]. Entre sus indicaciones se exigía la puesta en conocimiento de los usuarios del uso de cookies en las páginas web así como la necesaria aceptación del usuario para poder insertar esas galletas en los navegadores.

El problema con Google estriba en que esa información se le da al usuario de una forma parcial y sin la claridad necesaria. Es cierto que se pone en conocimiento de los usuarios que se almacenará determinada información relativa al uso que se haga de los servicios, y que el usuario es notificado de que se le instalarán cookies que permitan ese almacenamiento. Pero también es cierto que al usuario se le está diciendo que con ello se pretende mejorar la experiencia de navegación, no se le está informando del uso posterior que se llevará a cabo con esa información, como tampoco se le está advirtiendo que esa información será cedida/vendida por la empresa a terceros. Así mismo tampoco se le informa sobre la permanencia de las cookies en el navegador o el número total de cookies que se instalan.

La "ley de cookies", como se llama a la ampliación de la Directiva sobre la privacidad y las comunicaciones electrónicas[78], ha permitido que los usuarios sean conscientes del uso de las cookies y tengan que aceptar su uso cada vez que se entra por primera vez en un sitio web. Así un usuario puede aceptar o no que una determinada página web utilice cookies para conocer los movimientos del usuario por el sitio. El problema con Google es que el usuario acepta este uso de cookies al aceptar las condiciones de uso de los servicios. Si se quiere hacer uso de los servicios de Google el usuario deber aceptar, entre otras cosas, el uso de cookies que podrían atentar contra su privacidad. No existe la posibilidad de no aceptar el uso de estas cookies de rastreo y poder utilizar los servicios de la compañía. O lo que es lo mismo, el uso de estos servicios viene determinado por la cesión que el usuario debe realizar sobre sus datos de navegación.

---

77 http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:l24120&from=ES. Consultado por última vez el 15 de septiembre de 2016.

78 https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/normativa_estatal/common/pdfs/Ley_34_2002.pdf. Consultado por última vez el 1 de septiembre de 2016

Podría decirse, a modo de resumen, que mientras Google afirma proteger la privacidad de sus usuarios a modo de acceso restringido de la información, esto es, protegiendo con claves de acceso, contraseñas, información cifrada y no individualizando la información que recoge y almacena, por otro lado genera y obtiene beneficios precisamente otorgando permisos a ese acceso a la información de sus usuarios. Cabe preguntarse entonces si el modelo de acceso restringido a la información es suficiente para proteger la privacidad de los ciberciudadanos ya que respetando esa restricción de acceso se puede proteger y vulnerar la privacidad al mismo tiempo. Por otra parte surge la cuestión de si el modelo de negocio de Google, este es, el de otorgar servicios gratuitos a los usuarios a cambio de tener acceso a su información de navegación es un modelo que permita mantener la privacidad en el ciberespacio, al menos desde el modo en que es entendida actualmente.

La respuesta a estas preguntas parte de nuevo de qué se entiende por información personal y hasta qué punto la privacidad de los cibernautas se ve comprometida porque Google gestione esa información en su propio beneficio. La propuesta de un nuevo sentido para el concepto de información personal, en el cual se deje fuera toda información relativa a la navegación del usuario resolvería el problema de la invasión de la privacidad pero dejaría sin resolver el problema de la injerencia en los dispositivos al introducir en éstos elementos, las cookies, que pueden no ser deseados por los usuarios y sentir ese acto como una intromisión en sus dispositivos y por extensión en su privacidad. Por otra parte, la exigencia por parte de los usuarios, ya sea en forma de instituciones, gobiernos u otro tipo de asociación significaría, casi sin lugar a dudas, de la pérdida de gratuidad de los servicios de Google, ya que como empresa privada su objetivo es conseguir beneficios y no simplemente ofrecer servicios gratuitos a sus clientes.

El modelo de privacidad como acceso restringido no es, en el ciberespacio, suficiente para proteger la privacidad de las personas. Se ha visto que pueden darse situaciones donde exista un acceso restringido pero que se vulnere la privacidad. Por otra parte, tampoco es posible afirmar que Google no proteja la privacidad de sus usuarios mediante este acceso restringido. Sin embargo, a la vista de la existencia de las cookies y del control sobre la accesibilidad a la información, no se puede decir que el modelo que sigue sea netamente beneficioso para la privacidad de sus usuarios. Así mismo, vuelve a surgir la duda sobre la adecuación del concepto de privacidad, pues parece que, hasta el momento, ninguna de las teorías permite salvarla cuando se trata de hacerlo en el ciberespacio.

5.8. Google y la privacidad en público

A lo largo de esta investigación se ha ido haciendo hincapié en la idea de una red, una Internet pensada como un espacio público y abierto. Público porque cualquiera puede preguntar, compartir, opinar y relacionarse en el ciberespacio. Evidentemente existen ciertas limitaciones: técnicas cuando se está en entornos remotos donde la conectividad es escasa o nula; económicas cuando no se disponen de los medios necesarios para la conexión; y cognitivas en la medida en que existe un mayor o menor grado de alfabetización digital. Sin lugar a dudas estas situaciones influyen en que el ciberespacio no sea un lugar igualmente accesible para todas las personas. Pero en la medida en que estas situaciones son solventadas, cada individuo, convertido en ciberciudadano, tiene la posibilidad de habitar casi cualquier parte de este espacio. Abierto porque es un espacio sin restricciones, en el sentido de no estar sujeto a cuestiones geográficas o temporales, por ejemplo. La comunicación instantánea, las conexiones entre dispositivos remotos o la ampliación de los márgenes de acción determinan ese carácter abierto del ciberespacio.

Con estas características, como espacio público y abierto, algunos autores han visto la necesidad de tratar el tema de la privacidad también atendiendo a estos dos aspectos. En su momento se ha hablado de la cuestión de la privacidad en público y se ha expuesto desde la perspectiva de dos autores, Tavani y Nissenbaum. Recuérdese que para Tavani era fundamental distinguir dos tipos de información personal. Aquella que podía considerarse no pública donde estarían los datos bancarios o médicos y aquella información pública, como podía ser la marca de la moto de una persona o el lugar de trabajo. La información no pública venía determinada por su carácter de información protegida normativamente. La información personal pública no estaba sujeta a esa restricción. Para mantener el grado comunicativo del ciberespacio, decía el autor, es necesario mantener esa distinción y atender a las situaciones dentro de las cuales se enmarca cada uno de los dos tipos de información personal y aplicarlas al ciberespacio.

Por su parte, Nissenbaum, desde una perspectiva filosófico legal, denunciaba la falta de un corpus teórico-práctico que analizase los procesos de gestión de la información digital. Proponía tres motivos principales de esa carencia. Un factor conceptual, derivado de la división entre los espacios público y privado; un factor normativo, relacionado con el primero y que exige la necesidad de elección entre ambos espacios apelando al conflicto que puede darse entre ellos si se pretende conciliarlos; y un último factor empírico, determinado por la falta de capacidad de la filosofía de

hacer frente a los nuevos planteamientos sobre las cuestiones tradicionales que las tecnologías digitales presentan.

La propuesta de Tavani, y como se verá más adelante también la propuesta de Nissenbaum, puede servir para apoyar los argumentos que se esgrimen en esta investigación sobre la necesidad de redefinir, no solo la privacidad sino también, el concepto mismo de información personal. Por otra parte remiten a la cuestión de la privacidad en Google como acceso restringido que se ha analizado en el capítulo anterior.

Cuando se ha analizado la privacidad como acceso restringido en Google, se han tratado aspectos que por un lado apoyaban y ratificaban ese modelo, como era el caso del uso de contraseñas o la creación de cuentas personales para verificar y mantener la privacidad de los usuarios. Por otro lado se han visto otro tipo de situaciones donde la compañía podría no estar respetando el acceso restringido a la información, ejemplificado en el uso de determinadas cookies por un lado, y por la venta de información personal de los usuarios por otro. Tomando el argumento de Tavani por el cual hay que diferenciar entre dos tipos de información personal cabe preguntarse si efectivamente el uso de cookies y la venta de datos personales de los usuarios constituye efectivamente una violación de la privacidad de los usuarios.

En su momento (páginas 155y ss.) ya se ha hecho referencia, cuando se ha hablado de las preguntas de seguridad para recuperar los datos de acceso a las cuentas de Google, a que determinada información que antes no se consideraba como información personal se había convertido en el ciberespacio en una información sujeta a las normas de la privacidad. Se había puesto el ejemplo del nombre de la madre, el de la mascota, el del primer colegio, etc. Desde la perspectiva de Tavani esto podría plantearse desde varios puntos de vista y las respuestas serían también diversas. El resultado de las mismas podría ayudar a determinar si Google protege o vulnera la privacidad de sus usuarios.

En primer lugar podría suponerse que la información personal de los usuarios no es pública. Esto conllevaría afirmar, siguiendo el argumento del autor, que en la medida en que no es pública debe estar sujeta a unas reglas que la protejan, que pasarían por restringir o controlar el acceso a dicha información. En este sentido, se interpretaría que el uso actual de cookies, el rastreo y análisis del tráfico web, la comercialización de la información de los usuarios, la personalización y todo aquello

relacionado con el uso de datos de los usuarios sería una violación de su privacidad. Este argumento llevaría al rechazo de la existencia de dos tipos de información personal puesto que no habría cabida a una del tipo pública en el ciberespacio. Sería necesario entonces preguntarse por la condición de la información personal que los usuarios hacen pública. Habría que pensar qué hacer con las redes sociales, los blogs, los comentarios, las imágenes, los vídeos, los documentos, etc., de todos los usuarios que, de un modo u otro, exponen en el ciberespacio. Todas las web y plataformas que permiten el uso de esa información personal estarían vulnerando la privacidad de los usuarios, privacidad y acceso que por otra parte habrían cedido voluntariamente. Los usuarios, efectivamente, dispondrían de mayor privacidad en la medida en que su información estaría protegida de un uso inadecuado de la misma pero perderían la capacidad de decisión sobre qué información quisieran hacer pública o no, puesto que, al no existir información personal pública, toda estaría sujeta a unas normas externas a sus propias decisiones, lo que repercutiría en la pérdida de libertades.

Por otro lado se podría afirmar que la información de los usuarios contenida en el ciberespacio es pública, en virtud del carácter del espacio donde se crea y gestiona. En este sentido, el uso de la información por parte de los motores de búsqueda, de los usuarios-productores y de cualquier actor de la red, no tendría que suponer un atentado contra la privacidad del usuario. No habría cabida para la normatividad en cuanto al tratamiento de los datos se refiere y los usuarios estarían indefensos ante el uso que pueda hacerse de su información personal, incluyendo en este caso los datos bancarios, los informes médicos, y cualquier tipo de información almacenada en el ciberespacio.

En este segundo caso la situación no resulta ser mejor que la primera. Un ciberespacio sin normas que rijan el uso de la información personal de los usuarios no parece ser un espacio seguro donde éstos puedan sentirse protegidos. Como comunidad y espacio social, el ciberespacio necesita de unas normas de convivencia que permite a los ciberciudadanos ejercer sus derechos y deberes en un marco seguro y normativo donde existan límites que permitan actuar libremente en él.

Tomando a Google como ejemplo, si se aceptase que no hay información personal pública, entonces Google estaría haciendo un uso indebido de esa información. Pero no sólo esta compañía, sino que el ciberespacio al completo estaría vulnerando, de un modo u otro, la privacidad de los usuarios. Contrariamente, si se afirmara que toda la información personal es pública, entonces no se le podría acusar de utilizar los datos en su propio beneficio. Pero, se ha visto que entender la información personal sólo desde una perspectiva no aporta ventajas para la preservación de la privacidad ni

tampoco para la seguridad del ciberespacio. Se debe, por lo tanto, mantener la existencia de dos tipos de información personal.

Surge entonces una tercera vía que afirma, efectivamente, que la información personal contenida en la red debe entenderse como pública y privada. Esta es la postura defendida por Tavani que, junto al concepto de situación propuesto por Moor, ayudaría a proteger la privacidad de la información personal no pública y desmarcaría la información personal pública del debate sobre la privacidad. Sin embargo, a pesar de que esta formulación parece ser la más adecuada para el ciberespacio, surgen algunas dudas al respecto que se muestra a continuación.

En primer lugar está la cuestión de especificar con más detalle qué se entiende, o qué tipo de información, debe ser considerada para cada una de las acepciones. En el caso aquí expuesto, el evidenciar la existencia de dos tipos de información personal no resuelve el problema del uso de datos personales por parte de Google para la obtención de beneficios. Tavani afirma que la información personal no pública es aquella relativa a los datos bancarios o médicos de los usuarios y es este tipo de información la de que debe ser protegida con privacidad. Sin embargo, en el debate sobre la privacidad se incluye otro tipo de información, como la conseguida mediante el rastreo del tráfico web y la relativa al comportamiento del usuario.

Si se pretende que esta información personal es de carácter privado, entonces toda la red esta vulnerando en cierto modo la privacidad de los cibernautas y no sólo la empresa escogida como ejemplo. Si, por otro lado, se considera que aquélla es de carácter público, entonces no hay motivos para suponer que Google atenta contra la privacidad de los individuos al hacer uso de esa información, aunque sea en beneficio propio.

Se podría argumentar que es aquí donde entra en juego el concepto de situación y afirmar que es en el contexto donde aparece esa información que ésta toma un carácter privado o público. Póngase como ejemplo la red social Linkdlin, orientada a empresas, negocios y profesionales. En ella, los usuarios se crean un perfil profesional donde, además de incluir su experiencia profesional, pueden añadir cualquier tipo de información personal que consideren relevante. En la medida en que esa información ha sido expuesta por el usuario y a fin de que otros profesionales o empresas puedan acceder a su perfil, esto es, para tener visibilidad, en esta situación la información personal es de carácter público. Supóngase, además, que un usuario cualquiera, además de incluir su currículum,

ha añadido sus aficiones, como puede ser jugar a la petanca. Como información pública, cualquiera tiene posibilidad de saber que a ese usuario le gusta jugar a ese juego. No parece surgir ninguna cuestión sobre la privacidad de los usuarios cuando éstos incluyen esa información de modo voluntario en determinados sitios web, cuando hacen de esa información personal una del tipo pública y el contexto apoya esa situación.

Sin embargo, si Google, a través del rastreo del tráfico y el comportamiento del usuario "descubre" que a este en concreto le gusta jugar a la petanca, vende esa información a los usuarios-compradores y le muestra publicidad relativa a este juego, entonces se considera que se está haciendo un uso indebido de datos personales de los usuarios y que se está atentando contra su privacidad.

No parece que esta situación sea del todo clara a la hora de definir la información personal como pública o privada, así como tampoco un buen método para saber en qué momento se está protegiendo o vulnerando la privacidad de los usuarios. En determinadas situaciones la misma información puede ser pública y en otras privada, su uso puede considerarse legítimo e ilegítimo. Este estado de cosas, desde el punto de vista aquí sostenido, no resuelve ni ayuda a la privacidad ni a la protección de los datos personales.

Siguiendo los argumentos aquí expuestos no sólo es necesaria una distinción clara y tajante entre estos dos tipos de información personal sino también una redefinición del concepto mismo de privacidad. Esta necesidad de pensar en nuevos términos la privacidad vendría a unirse a ese factor empírico al que hace referencia Nissenbaum (página 98). La filosofía debería ser capaz de avanzar con las tecnologías digitales, adaptarse a los nuevos modos en que los individuos se relacionan con el mundo circundante y con los demás individuos para seguir aportando marcos de referencia desde los que habitar el ciberespacio. Ambas teorías, la asunción de dos tipos de información personal y la superación de la dicotomía entre espacio público y privado, junto con una filosofía capaz de superar los límites de sus propios supuestos, combinadas con la idea de una privacidad digital, podrían ayudar a solventar algunos de los problemas éticos que hoy surgen en el ciberespacio, como es el caso de la privacidad y del uso de datos personales que aquí se trata.

Desde la perspectiva de Google se podría afirmar que efectivamente la compañía apoya la idea de dos tipos diferentes de información personal. De hecho, Google distingue entre tres tipos de

información personal. Sin orden de importancia en esta exposición, la primera sería aquella información de carácter no personal que incluye información que Google "registra de forma que no refleje ni haga referencia a un usuario al que se pueda identificar de forma individual". Entre estos estarían los datos de navegación concretos, como puede ser el tráfico web de un determinado usuario, el uso que hace de la red, los medios que utiliza para navegar, y en general todo aquello que tiene que ver con su comportamiento en el ciberespacio. En segundo lugar estaría aquella información personal

> [...] proporcionada por los usuarios que permite identificarlos personalmente, como el nombre, la dirección de correo electrónico, la información de facturación u otro tipo de datos que Google pueda relacionar de manera razonable con dicha información como, por ejemplo, los datos asociados a tu cuenta de Google.

Por último distingue de las anteriores una información confidencial que "se incluye en una categoría especial por estar relacionada con datos médicos de carácter confidencial, información sobre la raza u origen étnico, creencias religiosas, ideología política o sexualidad".

De entre estos tres tipos de información personal, sólo aquella que Google no considera como información personal es compartida con los usuarios-productores. La información personal y la confidencial son respetadas por Google del mismo modo que se respetan fuera del ciberespacio. Dentro de esta categoría, además de los datos personales, estarían las contraseñas o claves de acceso, así como los datos relacionados con las finanzas de los usuarios, como puede ser el uso de GoogleWallet[79].

Este tipo de información ha sido siempre tratada como información personal, en el sentido de confidencial. La normatividad indica aquí que no es posible conocer el número de acceso a las tarjetas de crédito de las personas, que las llaves de las casas particulares son de uso exclusivo de los habitantes o que el correo personal no debe abrirse. Salvo que los titulares accedan a ofrecer ese tipo de información, las normas de convivencia indican que se ha de respetar la privacidad en este contexto. Y así es como trata Google la información relacionada con las claves de acceso y con el

---

[79] GoogleWallet es el sistema de pago móvil de la compañía que permite, entre otras cosas, el almacenamiento de tarjetas bancarias en los dispositivos móviles de los usuarios para realizar cualquier tipo de transacción monetaria. para más información véase https://www.google.com/wallet/

pago mediante sus aplicaciones así como la información que define confidencial. No existe la venta de información personal no pública de los usuarios por parte de Google.

Atendiendo a la diferencia entre los dos tipos de información personal y retomando la idea de situación propuesta por Moor y recogida por Tavani se ha visto que existen situaciones que permiten hablar de pérdida de privacidad y violación de la privacidad. Ambas situaciones se parecen pero difieren en la normatividad implícita en ellas. La pérdida de privacidad, como sería el caso que proponía Moor de ser descubierto en la cima de una montaña, no significa necesariamente una violación de la privacidad. Es posible que exista una pérdida de privacidad pero no una violación. Esta diferencia es fundamental para tratar la privacidad desde la perspectiva de Google.

Podría decirse que en la medida en que Google tiene acceso al correo personal de sus usuarios, de algún modo está teniendo acceso a una parte de la información personal no pública y que su uso podría entenderse como una violación de la privacidad. En cierta manera así es. Pero la cuestión no estriba en que Google tenga acceso a los correos electrónicos personales, ya que este acceso es parte de los servicios y los beneficios de este modo de comunicación interpersonal, como puede ser la capacidad de recuperación de los mensajes. El problema podría aparecer cuando la compañía utilizase la información contenida en aquéllos para proporcionar publicidad personalizada o que fueran mostrados al público. La exposición pública de la información contenida en los mensajes sería una violación de la privacidad en la medida en que esa información está protegida por unas normas que condenan su propagación. La cuestión de la publicidad personalizada basada en los mensajes personales crea mayores dificultades de análisis.

Si el uso de la información contenida en un correo personal es utilizada por la compañía para enviar publicidad relacionada con el contenido del mensaje podría decirse que se está haciendo un uso inapropiado de ese acceso a la información ya que se debería entender ese contenido como información personal no pública. Sin embargo también podría clasificarse dentro de lo que Google considera información no personal, si la información del mensaje se transmite de forma que no pueda relacionarse con el usuario en cuestión y en este sentido no habría violación de la privacidad, pero sí pérdida.

Imagínese que una usuaria escribe un correo electrónico informando a sus amigos que se ha quedado embarazada. A su vez comienza a realizar búsquedas sobre maternidad, crianza de hijos,

ginecólogos y tocólogos de referencia, tiendas de ropa de premamá, etc. A través de las cookies y otras herramientas de rastreo, la personalización de los resultados de búsqueda y la publicidad, así como las estadísticas relacionadas con el tráfico web, esa persona empezará a recibir publicidad relacionada con toda esa información que ha dejado en la red. Es posible también que esa publicidad esté relacionada con el mensaje que envió a sus amigos informando de la noticia. Pero a diferencia de su rastro o huella en la red, en este caso es difícil saber en qué medida ha afectado ese correo en la publicidad aparecida.

No se está diciendo aquí que no se haya utilizado, tan sólo se está afirmando que no es posible saber en qué medida los datos de los correos electrónicos son utilizados para el uso de la publicidad y si resulta relevante para la privacidad de los usuarios el uso anónimo de información personal para la personalización de la publicidad. En cualquier caso este hecho pone de relieve la necesidad de una ética en Internet que permita determinar de forma clara cuándo y por qué motivos la información personal puede ser utilizada. La información contenida en los mensajes podría tener el mismo tratamiento que la información confidencial. En primer lugar porque es información personal no pública. Es un mensaje entre dos o varias personas que se ha decidido transmitir por este medio y no por otros canales públicos en la red como podrían considerarse las redes sociales. En segundo lugar porque, del mismo modo que abrir el buzón de correo de las personas se considera un acto de violación de la privacidad de las mismas, utilizar el correo electrónico, en tanto conocer su contenido y actuar en consecuencia para enviar publicidad personalizada a los usuarios debería estar sujeto a las mismas reglas de conducta. Y por último porque la información contenida en los mensajes electrónicos puede contener información confidencial.

Póngase el ejemplo de que ese mismo mensaje notificando el embarazo de una persona lo envíe una adolescente desde el ordenador o un dispositivo compartido por todos los miembros de la familia. En él la noticia es transmitida como un inconveniente y consulta con sus amigas y amigos su deseo de abortar. Puede que las búsquedas que haga no tengan que ver con el cuidado de los hijos sino con las posibilidades de aborto en la sanidad pública, la legislación actual sobre los supuestos legales, las clínicas privadas y los precios, y la consulta en blogs sobre opiniones de otras embarazadas que desean interrumpir el embarazo. La publicidad relacionada con el mensaje y con las búsquedas realizadas, al igual que pasaba en el ejemplo anterior, estarán relacionadas con el contenido del mensaje y del historial de navegación por lo que se debe suponer que será publicidad encaminada a ofrecer posibilidades de aborto.

El hecho que otros miembros de la familia que utilizan el dispositivo puedan acceder a esta información debido a la publicidad basada en las búsquedas y al uso de la información contenida en los mails enviados supone una pérdida y una violación de la privacidad en la medida en que esa información, considerada como información personal no pública, y en términos de Google como información confidencial, ha sido utilizada sin el previo consentimiento de la parte afectada. De nuevo surge la necesidad de definir la información personal pública y privada así como el alcance de ambas. Por otro lado sería positivo para los ciberciudadanos, para el ciberespacio y la ciberética, así como Google que ésta redactara una Política de privacidad más clara y transparente respecto al uso de la información de los usuarios.

Existe, sin embargo, otra teoría de la privacidad que podría negar esta pérdida o violación de la privacidad y afirmar que esa información, en tanto ha quedado por escrito, esto es, ha sido documentada, ha dejado de ser información sujeta a las reglas de la privacidad. Este argumento, desarrollado por William Parent sostiene que la privacidad debe ser entendida como relativa a la información personal no documentada. Desde esta perspectiva, toda información contenida en el espacio pasaría a considerarse información personal pública.

5.9. Google y la privacidad como conocimiento de información personal no documentada

En su momento se ha señalado a William Parent y su propuesta sobre la privacidad como la teoría más cercana a la hora de entender la privacidad en el ciberespacio. Esta cercanía o adecuación se debe a varios motivos. El primero de todos, aunque no el más importante, es la centralidad del contenido por encima del control. En segundo lugar está la idea de una información personal basada en un acto consciente de revelación de determinada información. En tercer lugar está la cuestión de la asimilación, según el autor, de la privacidad como sinónimo de libertad. Por último surgía la idea de una invasión de la privacidad injustificada que remite directamente a la posibilidad de que existe una invasión de la privacidad justificada.

Como se recordará, la definición de Parent sobre la privacidad no versaba sobre el control o el acceso a la información, sino sobre la condición de que una persona mantuviera cierta información personal alejada del conocimiento de otros. Aquello que consideraba como información personal estaba la relativa a los hábitos sexuales, el tamaño de los genitales, el estado emocional de las pareja, etc. Si bien es cierto este tipo de información actualmente puede no verse como información

personal, sí que permite tener una idea de cómo entendía el autor este tipo de información. Así mismo, incluía dentro de esta categoría determinada información que podría ser tenida como privada en virtud de cuestiones subjetivas. Habría personas que, debido a una sensibilidad hacia ciertas características de sí mismas, decidieran tener cierta información en el ámbito de lo privado. La talla, el peso o la altura, por ejemplo, estarían dentro de esa información sensible.

Su definición de privacidad, basada siempre en información perteneciente a los hechos, partía de la idea de entender el concepto de información personal como aquella que la persona en cuestión decide no revelar, y de hacerlo, hacerlo a un grupo reducido de amigos y allegados. Negaba la definición de privacidad relacionada con el control o acceso sobre la información apelando a las situaciones en las que las personas decidieran libremente renunciar a su privacidad.

Los motivos por los que se desean ciertos grados de privacidad eran, para Parent, tres. El primero de ellos tenía que ver con el poder que se puede ejercer sobre alguien del cual se tiene información personal. El segundo era la intolerancia de algunos individuos sobre modos de pensar diferentes. El tercer motivo, relacionado con el primero, tenía que ver con el respeto a las personas en sí mismas que conlleva permitir mantener ciertos márgenes personales o privados que impidan utilizarlas como medios y no como fines en sí mismas.

Proponía una batería de preguntas por las cuales se puede saber, o al menos someter a prueba, si está sucediendo una invasión justificada de la privacidad de los individuos. Recuérdese que su objetivo no era negar toda acción contra la privacidad sino más bien demarcar las situaciones en las que una invasión de la misma podía estar justificada. Por medio de este examen la privacidad, lejos de quedar limitada, saldría reforzada.

Antes de comenzar la puesta a prueba de Google partiendo de las preguntas que propone Parent no estaría de más un par de cuestiones sobre el concepto de información personal como información personal no documentada. Se ha visto cómo este tipo de información personal parte de la idea que la persona a la cual pertenece dicha información realiza todas las acciones posibles para que aquélla se mantenga fuera del alcance del público general o, al menos, se limite a un grupo muy pequeño de allegados.

El autor ponía como ejemplos de este tipo de información temas relacionados con el tamaño de los genitales, la altura, el peso, la felicidad marital, etc. Ejemplos todos ellos de un tipo de información que determinadas personas pueden considerar como información sensible. En 1983, momento en que Parent publicaba el artículo al cual se hace referencia, podía resultar fácil conseguir que ese tipo de información se mantuviera alejada del público, y sobre todo alejada de la posibilidad de documentar tal información.

Actualmente, la capacidad de almacenar información y la variedad de dispositivos que permiten la captura de información en una variedad muy amplia de formatos dificultan o disminuyen las posibilidades de que los individuos tengan información personal no documentada, lo que significa, siguiendo los argumentos de Parent, que dispongan de privacidad.

Póngase como ejemplo una persona que considera que su altura entra dentro de la categoría de información personal sensible y que prefiere mantener indocumentada esa información sobre su persona. Está preocupada por ese aspecto de su cuerpo y busca apoyo y consuelo entre las personas cercanas a ella. Así mismo, preocupada, busca información en la red relativa a los modos de disimular su altura. En este caso están sucediendo, al menos, dos situaciones que le impiden mantener ese dato personal como privado. En primer lugar está permitiendo el acceso a esa información a terceros, lo que le dificultará el control sobre esa información ya que una vez expuesto a terceros pierde la capacidad de controlar la diseminación de la informació. En segundo lugar, al realizar búsquedas sobre los modos de disimular su estatura está, en cierta forma, documentando esa información que deseaba mantener como información personal. En este sentido, no sólo está difundiendo esa información sino que, siguiendo los argumentos del autor, está renunciando a la privacidad. En la medida en que renuncia a esa privacidad está renunciando a su vez a reclamar cualquier norma que impida la difusión de esa información.

La cuestión fundamental de la privacidad como información personal no documentada aplicada en el ciberespacio estriba en que, por definición, cualquier tipo de información que se introduzca en la red pasa automáticamente a convertirse en documentada. Como tal, pierde toda capacidad de mantenerse en el reino de lo privado y cualquier tipo de restricción en su difusión es una aplicación injusta de las normas que rigen la privacidad.

Habría que analizar en qué medida es justo o no, o si tiene que ver con la justicia, que todas las búsquedas e información que se introduzca en la red pasen a ser información documentada. Podría decirse que el hecho que una persona busque información sobre cómo disimular su altura no significa que esté cediendo esa información al ciberespacio y que ésta pueda ser utilizada indiscriminadamente. Pero ciertamente así funciona el ciberespacio. Éste se compone de toda la información introducida y compartida en él. Desde la perspectiva de la privacidad entendida como información personal no documentada el mejor modo de mantener aquélla es no exponer ésta en el ciberespacio, de otro modo pasará a ser información personal documentada y por ende, susceptible de ser difundida.

Véase ahora cómo podría responder Google a las preguntas que plantea Parent para saber si la privacidad está siendo invadida de un modo justificado o no. Hay que señalar que no es posible conocer las respuestas que la propia compañía daría a estas preguntas. Las respuestas expuestas forman parte de un ejercicio en el cual se intentan responder partiendo de la información contenida en la Política de privacidad de Google y en su modo de actuar ante ciertas situaciones. Para realizar esta prueba se pondrá como ejemplo lo más parecido que se pueda entender en el ciberespacio como información personal no documentada, a saber, el rastreo del tráfico y el seguimiento de los usuarios. Si bien es cierto que este tipo de información, la huella digital, no cumple, estrictamente hablando, con la definición de información personal no documentada, ésta parece ser la que más problemas causa a la hora de hablar de privacidad en el ciberespacio. Por otra parte, como información generada por los usuarios de un modo, que podría decirse, involuntario, y recogida, almacenada y gestionada por Google sin la participación y el consentimiento continuo de los usuarios, resulta ser la mejor opción a la hora de realizar este análisis.

5.9.1. Motivos de búsqueda de información personal no documentada

La primera pregunta que plantea Parent tiene que ver con los motivos por los que se busca información personal no documentada. En el caso del análisis que aquí se realiza la pregunta podría reformularse en el sentido de qué razones esgrime Google para rastrear el uso de la red y el tráfico generado por los usuarios. Se ha dicho en su momento que este tipo de seguimiento del usuario se realiza a través de las llamadas cookies o galletas informáticas. Se ha visto también cómo muchas de éstas permiten que el usuario tenga una experiencia más satisfactoria que sin ellas. Posibilitan la creación de perfiles únicos y personalizados al recordar las preferencias de navegación como el idioma, la navegación, las contraseñas. Así mismo permiten almacenar información relativa al

historial de navegación del usuario haciendo que éste pueda acceder a sitios web que haya visitado con anterioridad o crear una memoria en un determinado sitio web para que el usuario pueda realizar compras. También se ha señalado que el rastreo y seguimiento del tráfico web son herramientas útiles para la detección de casos que vulneren la legalidad o la seguridad, como las redes de pedofilia, terrorismo, comercio humano, etc.

Todas estas funciones necesitan para su correcto funcionamiento el acceso al tráfico y al uso de la red que hace cada usuario. En este sentido se puede decir que estas tareas son llevadas a cabo a través del uso de información personal no documentada de los usuarios. ¿Suponen estas acciones un abuso de la privacidad de los usuarios? ¿Qué motivos esgrime Google para hacer uso de ese tipo de información? Los motivos son múltiples y cada uno de ellos tiene una justificación por parte de la compañía.

El primero de todos, y el más fundamental, es un motivo técnico. Google y el PageRank, y general los motores de búsqueda, funcionan rastreando la red, clasificándola y ordenando la información en orden de relevancia y presentándola en forma de resultados de búsqueda. Parece que este tipo de funcionamiento no crea problemas al hablar de la privacidad. Sin embargo, cuando se siguen los mismos mecanismos con los usuarios, mediante el rastreo y análisis del tráfico web y la personalización de contenidos, incluida la publicidad mostrada, para clasificar, ordenar y presentar la información de los usuarios, la privacidad aparece como escollo principal para este funcionamiento técnico. Pero si se desea que Google, y los motores búsqueda en general, ofrezcan información relevante, es necesario el uso de esas técnicas y el debate sobre la privacidad debería quedar al margen. Por lo tanto, desde la perspectiva técnica, se podría decir que existen motivos suficientes para el uso de información personal no documentada, en la medida en que forma parte esencial del modo de gestión de la información.

Otro motivo que debe tenerse en cuenta es la obtención de beneficios por parte de Google a través del uso de este tipo de información, a cambio de herramientas y servicios que hacen del motor ser el preferido por los cibernautas. Como se ha dicho en repetidas ocasiones, la fuente principal de ingresos de la compañía es la gestión de la información personal no documentada de los usuarios. Éstos, a cambio, tienen a su disposición diversas aplicaciones, servicios y mecanismos que les permiten navegar por la red de un modo cómodo, eficaz, personalizado y gratuito. Puede entenderse que este motivo no es suficiente para la pérdida de privacidad por el uso de ese tipo de información.

En este caso, el usuario siempre tiene la posibilidad de navegar por el otro tipo de red, la que se ha denominado red profunda. Nada le obliga al cibernauta a permanecer en la red superficial y a hacer uso de los servicios de Google. Sin embargo, si se mantiene en la red superficial, deberá tener presente que, en virtud al primer motivo, por una cuestión técnica, independientemente del motor de búsqueda que use, su información personal no documentada será rastreada y gestionada para el mantenimiento del ciberespacio.

En la medida en que estas herramientas que ofrece Google pueden bloquearse o aceptarse no se puede decir que sea un uso injustificado de la privacidad; es el usuario quien tiene los mecanismos, ofrecidos por Google, para acceder o no a ese uso de la información personal. Ahora bien, cuando el uso de información personal se hace sin el consentimiento explícito e informado de los usuarios, se vende a terceros, se mantiene por un tiempo indeterminado e indiscriminadamente entonces se podría hablar de un uso injustificado de esa información.

Podría mostrarse otro motivo por el cual Google hace uso de esa información personal no documentada. Éste es del tipo subjetivo y difícilmente comprobable empíricamente, aunque igualmente válido como se verá a continuación. El usuario medio, que por medio debe entenderse aquél que hace un uso de la red de modo cotidiano, con un conocimiento técnico limitado al uso simple de la red, desea que se le muestre la información de un modo personalizado, acorde a sus intereses, aficiones y preferencias. Así mismo prefiere una navegabilidad sencilla, rápida y gratuita. Su preocupación principal no es la privacidad de la información sino el interés y sencillez de la información mostrada.

Google dispone de una herramienta denominada Google Trends en la que se puede ver qué información han buscado los internautas, ya sea por año, por temática, por formulación de búsquedas, etc. Si se analizan las tendencias de 2015 en España, por ejemplo, se verá qué tipo de información busca el usuario medio y cuáles son las preocupaciones de los cibernautas españoles. Aquí se van a mostrar sólo los primeros puestos de las diferentes clasificaciones:

1. Los términos que más crecieron: Gran Hermano 16.
2. ¿Cómo ser...?: Cómo ser feliz.
3. ¿Qué pasaría si...?: Qué pasaría si Cataluña se independizara.
4. ¿Cómo evitar...?: Cómo evitar los gases.
5. ¿Cómo saber...?: Cómo saber si estás embarazada.

6. ¿Qué hacer cuando...?: Qué hacer cuando estás aburrido[80].

Los intereses del cibernauta medio están encaminados a una red útil para sus intereses y éstos se conocen y se muestran en forma de resultados a través de las herramientas de rastreo y monitorización del tráfico web, de la personalización de contenidos, de la muestra de publicidad relevante, etc. Se podría decir entonces que uno de los motivos por los que Google hace uso de la información personal no documentada de los usuarios es para mostrarles y ofrecerlas la información (y la red) que desean ver.

5.9.2. Propósitos de uso de información personal no documentada

La segunda pregunta que ha de formularse es saber si el propósito de ese uso de información es legítimo e importante. Esta cuestión, que desde este planteamiento puede entenderse como dos preguntas diferentes, una sobre la legitimidad y otra sobre la importancia, deben responderse por separado. En primer lugar, desde la perspectiva de Google, podría decirse que para la compañía es ambas cosas, legítimo e importante. Legítimo porque es el modo en que pueden ofrecer servicios gratuitos a sus usuarios al tiempo que obtiene beneficios. Así mismo supone la posibilidad de desarrollar y crear nuevas herramientas, que de nuevo sean gratuitas para sus usuarios y que le reporten ganancias mediante la información conseguida de su uso. Desde la perspectiva de la importancia, el uso de este tipo de información es importante para Google porque supone su principal fuente de ingresos.

Desde el punto de vista del usuario (al menos desde el usuario-comprador) la respuesta puede ser diferente. La legitimidad desde la perspectiva del usuario debería entenderse también desde el carácter gratuito de los servicios de los que dispone. Sería injusto pensar que una compañía privada que ofrece unos servicios gratuitos no debiera conseguir beneficio de ellos de algún modo. Sería interesarte saber en qué medida los usuarios aceptarían pagar por utilizar las herramientas de Google a cambio de proteger su privacidad. Puede ser que algunos internautas estuvieran de acuerdo en pagar una cantidad de dinero porque su privacidad fuera respetada. Pero habría que suponer que de ser así, estos usuarios estarían navegando en la red profunda de un modo gratuito. Así mismo, no sería extraño pensar que muchos otros no estarían a favor de tener que pagar por esos servicios y preferirían ceder ámbitos de su privacidad por el mantenimiento de la gratuidad de aquéllos. El ejemplo más claro son las aplicaciones para dispositivos móviles, como los teléfonos o

[80] https://www.google.es/trends/topcharts#date=2015

las tabletas. Algunas de las aplicaciones más conocidas, como podrían ser las de mensajería instantánea o las de redes sociales, suponen para el usuario la aceptación de una serie de condiciones que implican una pérdida de privacidad, como el acceso a la agenda de teléfono, a la cámara, la ubicación, el micrófono, la instalación de herramientas de rastreo, etc. En el uso de estas aplicaciones, el usuario no parece preocuparse por toda esa información cedida a la empresa o la compañía proveedora del servicio sino por la privacidad que pueda perder en contacto con otros usuarios de la aplicación.

Cuando alguna de estas aplicaciones ha pretendido volverse de pago se han levantado las voces de los usuarios y han crecido las alternativas gratuitas. Por otra parte, cuando se establecen nuevos mecanismos para que los usuarios sientan que se les protege ante las intromisiones, ocultando las horas de conexión, limitando el uso de marcas que puedan identificar si un mensaje ha sido leído o no, etc., la comunidad de usuarios alaba tales acciones. Sin embargo, que esas mismas empresas tengan acceso ilimitado a su información no parece generar ningún debate sobre la privacidad por lo que, si se atiende a las preocupaciones expuestas por los propios usuarios, parece que éstos están más preocupados de la gratuidad y de la vigilancia de otros usuarios que de las propias compañías que almacenan y gestionan su información. Se vuelve aquí a unas de las características de la privacidad analógica, que no tenía en cuenta los intereses de los propios usuarios y pretende un modelo de privacidad que tal vez ya no encaja con aquellos a los cuales se intenta aplicar.

En cuanto a la importancia desde el punto de vista del usuario la respuesta no está clara. Éste, desde la perspectiva de la publicidad, puede preferir que se le ofrezca publicidad relacionada con las búsquedas que realiza y en definitiva con sus intereses. También resulta más positivo para la experiencia del usuario que la publicidad se muestre de un modo que no sea molesto para la navegación. Desde este modo, la importancia del uso de esa información puede ser importante. Ahora bien, también hay que decir que la publicidad en sí no es importante para el usuario, al menos para el usuario-comprador. Si la publicidad estorbaba en otras plataformas como la televisión o la radio, y el zapeo surgió como mecanismo de evasión de los espacios publicitarios, el hecho que en Internet sea una publicidad menos invasiva y más personalizada no implica que sea más aceptada.

La importancia del uso de información personal no documentada para los usuarios se topa así mismo con la dificultad de conocer las inquietudes de todos ellos en su conjunto. Habría que

analizar en qué medida y en qué cantidad los usuarios ponen en práctica todas las herramientas de las que disponen, tanto las que ofrece Google como otras existentes, para proteger su privacidad ante el uso de este tipo de información personal. Podría resultar que los usuarios, ya sea por desconocimiento técnico, por pereza o por saberse inútil, no aplicasen los mecanismos a su alcance para proteger su privacidad. Este hecho remitiría, otra vez, a esa tercera característica que se proponía para la privacidad analógica. Recuérdese que era una privacidad que no tenía en cuenta los deseos o intereses de las personas interesadas. Podría suceder que los usuarios estuvieran más interesados en mantener la usabilidad, los servicios gratuitos y la comunicación actual que en proteger determinados aspectos de su privacidad, como se ha mencionado más arriba al hablar de las aplicaciones móviles.

Intentar mantener ese concepto de privacidad, alejada de los intereses reales de los usuarios y obligar a las empresas y a los usuarios-productores, desde teorías que imponen un modo analógico de entender la privacidad, parece ser la crítica que hace Nissenbaum a la filosofía, la incapacidad de adaptarse a las tecnologías digitales, encasillada en viejos modos que le impiden hacerse fuerte y tener una aplicación real dentro del ciberespacio. Es necesaria, desde el punto de vista aquí defendido, una filosofía, una ética y una privacidad verdaderamente digitales, que sepan rehacerse y adaptarse a este entorno, que sean capaces de abandonar las ideas que ya no encajan y que refuercen aquellas que pueden ayudar al ciberespacio a ser un lugar ético, crítico y racional.

5.9.3. Importancia del conocimiento adquirido

La tercera pregunta que se plantea tiene que ver con la importancia del conocimiento obtenido por la invasión de la privacidad para la legitimidad del propósito. Los propósitos tenían que ver, por un lado con la mejora de la experiencia del usuario ofreciendo servicios que mejoren la navegación y por otro lado, con la obtención de beneficios a través de la gestión y la venta de información personal. Saber cuánto tiempo ha estado un cibernauta en un sitio web, qué anuncios ha clicado, qué intereses tiene y en general de qué modo navega por la red tiene, sin lugar a dudas, una importancia capital para Google. En primer lugar porque le permite tener un conocimiento sobre la aceptación de las herramientas y los servicios que desarrolla. En segundo lugar porque le ofrece estadísticas que permiten maximizar sus esfuerzos y los de los usuarios-productores. En tercer lugar porque le permite ofrecer al usuario una mejor navegabilidad en tanto personalización de la experiencia.

Las pruebas y aceptación de los servicios, las estadísticas y la maximización de los esfuerzos son elementos fundamentales para el correcto desarrollo de cualquier actividad y por ende de la tecnología e Internet. Así mismo, ofrecer determinadas herramientas para que los usuarios mantengan una satisfacción, uno de los propósitos del uso de información personal no documentada, es una razón válida para que se recabe información. Ahora bien, todos estos argumentos pueden no ser suficientes a la hora de justificar el modo en que esa recolección se realiza.

El problema fundamental al que se enfrenta la ciberética, el ciberespacio en general y todas los actores de la red, parte precisamente de la manera, y su justificación, en la que la información personal no documentada se recolecta. Este concepto de recolección, que Nissenbaum también utiliza, no es casual. La manera en la que la información personal no documentada de los usuarios es almacenada indica una acumulación de esa información. No se realiza tan sólo para mejorar los servicios, realizar estadísticas y permitir el buen funcionamiento de la red en general, sino que se hace de una forma indiscriminada y basada en el hecho de que la propia tecnología, así como la escasa legislación al respecto, lo permite.

La recolección de datos no es algo que haya surgido con las tecnologías digitales. Las bases de datos o la acumulación de información sobre un determinado asunto es una tarea que se ha llevado a cabo desde la antigüedad. Si se entiende por datos cualquier tipo de información que pretenda la conservación de dicha información, se puede decir que desde las primeras formas de expresión cultural se ha perseguido un modo de almacenamiento y recolección de información, en tanto modo de transmisión cultural.

Lo que sí han permitido las tecnologías digitales es una acumulación y recolección de datos de un modo sin precedentes hasta su aparición. La rapidez, facilidad y la expansión que permiten estas tecnologías ha supuesto que el uso de los datos se haga de una forma indiscriminada. Indiscriminada en la medida en que aunque no existan motivos actuales para el almacenamiento de información, el hecho de poder hacerlo determina que efectivamente se almacene. El cambio de perspectiva en este sentido es notable desde los comienzos de las bases de datos. Cuando era necesario llevar un control sobre el número de individuos que formaban la comunidad, un inventario sobre las pertenencias de un pueblo, una contabilidad sobre los productos obtenidos en una cosecha concreta, etc., el almacenamiento de esa información tenía un objetivo concreto.

Actualmente, la facilidad con la que esa información puede ser almacenada implica que no tenga que haber un objetivo concreto para esa recolección o lo que es lo mismo, la importancia del conocimiento adquirido no es el objetivo y la justificación de esa recolección. Cuando Edward Snowden denuncia que el gobierno de Estados Unidos realiza vigilancias masivas de sus ciudadanos y de otros países apunta en esa dirección. La vigilancia no se lleva a cabo sobre posibles criminales, terroristas o gobiernos que puedan poner en peligro la seguridad nacional sino que, en virtud de la posibilidad de hacerlo, se vigila y almacena información indiscriminadamente a la espera que pueda ser útil en el futuro.

La información personal no documentada que pueda recolectar y almacenar Google sobre sus usuarios no es una cuestión exclusiva de la compañía, sino relativa al funcionamiento propio de la red, las tecnologías digitales y el almacenamiento masivo de datos. La justificación sobre el conocimiento adquirido a través de esta información por parte de Google resultará insuficiente, del mismo modo que lo es para el resto de empresas y para la red misma. Estará justificada con el propósito de mejorar los servicios de los usuarios así como para la creación de bases de datos que permitan una mejor navegabilidad, pero el modo de recolección masiva de datos sin un objetivo concreto no tendrá justificación posible más allá de la propia posibilidad de hacerlo y por lo tanto será una acción injusta.

En cualquier caso es necesario señalar que no toda la recolección masiva de datos significa necesariamente una pérdida de privacidad y menos aun un problema a resolver. La práctica de este tipo de almacenaje y uso de la información permite realizar cruces de datos que mejoren muchos servicios beneficiosos para las personas. Así, que un hospital haga uso de este tipo de recolección permite que éste pueda mejorar sus recursos ya que dispone de información sobre los momentos donde más equipo médico necesita, el material necesario para cada época o estación, la maximización de las instalaciones como quirófanos o camas disponibles, la realización de balances sobre la incidencia de determinadas enfermedades en segmentos de población concreta, etc. La agricultura, por ejemplo, puede cruzar datos meteorológicos con las herramientas de las que dispone como los sistemas de riego, el número de invernaderos disponibles o el coste de producción de determinados productos para mejorar la productividad y rentabilidad de sus cosechas. Las empresas bancarias, las energéticas, las compañías telefónicas o las de textil pueden utilizar información relativa a la compra venta de productos, el tipo de público objetivo o los modelos de cliente para ofrecer mejores servicios, modificar los precios y proponer ofertas adecuadas para cada situación.

Todas estas acciones vienen determinadas por la posibilidad de gestionar y combinar una cantidad considerable de datos, información que se consigue a través de la adquisición de información personal no documentada. En algunos momentos y para unos propósitos, esto es, en función de la importancia del conocimiento adquirido a partir de esa recolección de información, parece que el uso de esa información supone una mejora en la calidad de vida de las personas y sería inadecuado considerarlo como algo negativo alegando que esos mismos beneficiarios están perdiendo, de algún modo, privacidad. Sin embargo, Google no es un hospital o un campo de trigo que alimenta a determinada población. Es una empresa privada que obtiene beneficios del uso de información personal no documentada de sus usuarios. La justificación de esa recolección vendrá determinada por la consideración que se tenga a la mejora de sus servicios y al mercado del comercio en línea, así como por la definición que de privacidad se tenga presente a la hora de analizar la situación.

Si se mantiene el concepto de privacidad actual y se afirma que la recolección de datos está suponiendo una pérdida injustificada de la privacidad, en la medida en que no existe justificación suficiente para tal recolección, habría que tener en cuenta que esa pérdida se está dando en todos los aspectos de la vida de los ciberciudadanos y no sólo de los usuarios de Google. Cierto es también que por ser una situación generalizada no se transforma en positiva y deja de ser menos perjudicial para la privacidad de los individuos. Siendo un problema sistémico cabe preguntarse si el problema radica en el propio sistema digital que permite ese almacenamiento masivo o si por el contrario la dificultad está en los criterios que se siguen para considerarlo injusto y/o negativo. Sea cual sea la respuesta, tanto si se afirma que es un problema de la tecnología misma como si se pretende que es una cuestión de la teoría que lo juzga, lo cierto que es la capacidad de almacenar información va a seguir estando ahí, se va a mejorar y se van a ampliar las posibilidades de almacenamiento, recolección y combinación de información. El hecho que pueda significar perder la privacidad de los usuarios y los ciudadanos difícilmente va a condicionar que la ciencia tecnológica avance en su capacidad de almacenar y procesar información. Por lo tanto habrá que buscar mecanismos que permitan su evolución sin que ello conlleve la pérdida total de privacidad. Esto pasa, desde el punto de vista aquí expuesto, por una reformulación del concepto de privacidad que, sin perder terreno, permita a los individuos sentirse seguros dentro del mundo digital.

5.9.4. Alternativas al uso de información personal no documentada

Parent plantea como cuarta pregunta para poner a prueba la justificación de la invasión de la privacidad preguntarse sobre las alternativas a la misma para adquirir información. Una

justificación para invadir la privacidad debe haber contemplado otras formas de adquirir conocimiento que sean las menos ofensivas para los actores implicados. Desde el ejemplo aquí tratado, la pregunta radica en saber en qué medida es ofensiva la adquisición por parte de Google de información personal no documentada. En segundo lugar si existen alternativas para la obtención de esos datos que no sea el modo actual.

Será mejor comenzar la reflexión partiendo de la segunda pregunta. Como se ha dicho en numerosas ocasiones, las tecnologías digitales han permitido la recolección y el almacenamiento de la información sin precedentes. Hasta la aparición de las computadoras y la digitalización de la información ésta debía ser almacenada básicamente en papel, en grandes ficheros almacenados en grandes superficies físicas. Cuando se necesitaba tener acceso a esos datos había que llegar hasta el lugar donde estuvieran almacenados, hablar con la persona o institución encargada de su custodia o disponer de una autorización para acceder a ellos, buscar entre los diferentes ficheros que pudiera haber en el espacio y finalmente encontrar la información deseada. Existían numerosos pasos, a veces prácticamente insalvables, que dificultaban o impedían el acceso a la información. Las tecnologías digitales han permitido que muchos de esos escollos se hayan convertido en inconvenientes más o menos molestos y en algunos casos hayan desaparecido del todo. El acceso a determinada información es actualmente una cuestión económica. Ya sea en forma de acceso tecnológico, de alfabetización digital o de posibilidad de pago para obtener acceso a esa información.

Ese almacenamiento y recolección de información sin precedentes ha supuesto a su vez una creación de datos también genuina de estas tecnologías. Nunca en la historia de la humanidad se había generado y almacenado tanta información en tan poco tiempo. Cada uno de los actores que intervienen en el ciberespacio, e incluso aquellos que no toman parte activa en él (los datos de una persona pueden ser digitalizados sin que ella participe directamente del ciberespacio), producen información que es almacenada en la red. En este sentido, preguntarse sobre las alternativas a la hora de obtener información personal no documentada tiene como respuesta una negativa. Ciertamente, no existen alternativas para el acceso de tanta información personal no documentada de tantas personas. De hecho, teniendo en cuenta que se ha comenzado este análisis afirmando que se debía entender por este tipo de información aquella relacionada con el tráfico y el uso de la red generada por los usuarios no sería posible acceder a esta información de otro modo que no fuera precisamente el medio actual, en tanto ésta pertenece por necesidad a este ámbito.

En cuanto a la ofensa o no del modo en que se recoge esa información la respuesta es relativamente simple. Esta recogida de datos se hace de un modo invisible y silencioso. De hecho, hasta que no se han tomado las medidas necesarias para que sea evidente, el uso de cookies, por ejemplo, resultaba desconocido para la mayoría de los cibernautas. Este sigilo con el que se almacenan los datos es poco ofensivo si se entiende por esto que no se hace de un modo público y vejatorio para los individuos. Por otro lado, sin embargo, es ofensivo en la medida en que se hace de un modo constante, masivo y en muchos casos sin el conocimiento informado previo de los interesados. Se podría argumentar que el rastreo de información sin el consentimiento de los individuos no significa que el hecho en sí sea menos ofensivo. En el caso de las cookies, el hecho de que se informe a los usuarios que se está utilizando su información y que ésta pueda ser compartida con terceros no disminuye la posible ofensa que supone que esa información vaya a ser distribuida por la red.

Ahora bien, el concepto de ofensa o la acción de ofender tiene que ver con un sentimiento de humillación, con herir el amor propio de las personas. Habría que analizar si los movimientos de los cibernautas en la red son tan importantes en términos de privacidad como para que éstos se puedan sentir humillados u ofendidos porque se rastree y almacene la información de sus movimientos en la red. Un paralelismo fácil podría ser la vigilancia masiva que se ha dado a lo largo de la historia en diferentes países y bajo diversos regímenes, casi siempre éstos de carácter totalitario. Resulta evidente que esas acciones llevadas a cabo por los gobiernos resultaban acciones ofensivas y humillantes para la población y sería difícil justificar cualquier tipo de acción de este tipo.

Sin embargo, la diferencia fundamental entre esos actos y la recolección de datos masiva de las tecnologías digitales, y en concreto de la recolección que lleva a cabo Google, es que esa vigilancia se hacía de forma personal e individual. Las personas eran vigiladas con nombre y apellidos y siempre bajo el prisma de encontrar posibles disidentes o personas contrarias al régimen que las llevaba a cabo y su objetivo era controlar, denunciar, detener y someter a los implicados y en este sentido, humillarlos. Google por su parte, al menos desde los argumentos que plantea, el almacenamiento de esa información lo hace de forma anónima, sin intención de señalar a nadie y menoscabar su libertad personal. Los motivos que esgrime son siempre “para ofrecer mejores servicios a todos nuestros usuarios”.

El problema, de nuevo, es que los intereses de los dos grupos de usuarios de Google son diferentes e incluso opuestos. Un acto conciliador por parte de la compañía, que podría tranquilizar a la

opinión pública, sería la creación de una Política de privacidad que diferenciara a ambos usuarios, que expresara de un modo claro cuándo está defendiendo los intereses de unos y de otros. De este modo se podría juzgar con mayor conocimiento de causa la justicia o no de la invasión de la privacidad. Hasta que esto no suceda es casi inevitable pensar, debido a la poca transparencia, que el modo en que se recoge información personal no documentada de los usuarios se está realizando de un modo ilícito, injusto o ambos.

5.9.5. Mecanismos para proteger la información personal no documentada

La quinta pregunta es fundamental para entender lo dicho en las líneas anteriores. Como Parent afirma a la hora de explicar su formulación "Question (5) pertains to the actual invasion of privacy itself. We can say that the right to privacy is violated by indiscriminate invasions and that these occur when insufficient procedural safeguards have been imposed on the techniques employed" (Parent, 1983, p.281).

La legislación en Internet no se ha desarrollado a la misma velocidad que la propia tecnología. Si bien es cierto que las leyes existentes han servido para incluir la ley dentro del ciberespacio, se ha dado también una imposibilidad, como afirma Manuel Castells, de llegar a acuerdos claros entre diferentes países implicados [81] . Así mismo los diversos intereses y la propia rapidez en la implementación de cambios en la tecnología han dificultado esa concordancia de tiempos.

El ciberespacio no es un lugar sin ley. La protección de datos personales es una de las cuestiones más destacadas en lo que a legislación digital se refiere. El tratamiento de datos personales así como su circulación por el ciberespacio suscitaron una preocupación temprana. En Europa la propia ley que regulaba el tratamiento de datos, y la transferencia de éstos entre estados miembros, sentó las bases de las normas que en este sentido debían regir el ciberespacio. Así, en 1995 se ratificaba la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Su objetivo era sentar las bases para la creación de un marco legal para la protección de las personas físicas en el tratamiento de datos personales y su libre circulación. En ella[82] se define el término "datos personales" como:

---

[81] http://www.uoc.edu/web/esp/launiversidad/inaugural01/experiencia.html

[82] Ésta y las siguientes citas están contenidas en el documento en cuestión que puede consultarse en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l14012

> Toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

y tratamiento de datos personales como:

> Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

A medida que avanzaban las tecnologías digitales y se asentaban como nuevo marco de convivencia, otras leyes tuvieron que llevarse a cabo, éstas más específicas, para el nuevo entorno social. Así, en 2000 se ratificaba la Directiva 2000/31/CE sobre determinados aspectos jurídicos, esta vez, relativos a ciertos servicios de la sociedad de la información y en concreto del comercio electrónico. En esta nueva ley no se modificaba la anterior respecto al tratamiento de datos personales puesto que,

> Dichas Directivas (95/46/CE) establecen ya un marco jurídico comunitario en materia de datos personales y, por tanto, no es necesario abordar este aspecto en la presente Directiva para garantizar el correcto funcionamiento del mercado interior, en particular la libre circulación de datos personales entre Estados miembros.

En España en concreto, esta ley europea tendrá su respuesta en la Ley 34/2002, que será llamada coloquialmente la “ley de cookies”. Entre otras cosas esta ley imponía a los sitios web informar a los cibernautas del uso de galletas informáticas y la necesidad de aceptación explícita de éstos a ese uso.

Todas estas leyes, que sin duda ha ayudado a que los cibernautas tengan unos derechos en el ciberespacio, resultan insuficientes a la hora de proteger efectivamente los datos personales como información personal no documentada. El problema fundamental es que estas leyes no impiden el

uso y el rastreo de este tipo de información sino que tan sólo determinan que el usuario debe estar informado de ese uso. Por otra parte la Política de privacidad de Google es clara a este respecto:

> Las leyes del estado de California (Estados Unidos) se aplicarán a cualquier litigio que se derive de estas condiciones o de los Servicios o que esté relacionado con los mismos, sin que tenga efecto las disposiciones sobre los conflictos de leyes. Tanto Google como tú aceptáis someteros a la jurisdicción exclusiva de los tribunales federales o estatales del condado de Santa Clara (California, Estados Unidos) para solucionar las reclamaciones derivadas de estas condiciones o de los Servicios o relacionadas con los mismos.

Dicho de otro modo, Google se rige por las leyes concretas de un país determinado y no por las determinadas por otros países, organizaciones o instituciones. No se puede negar que existen mecanismos que salvaguarden la privacidad de los usuarios de Google, en la medida en que se han desarrollado leyes que permiten esa protección. La propia compañía dispone de herramientas y mecanismos que permiten al usuario cierto control sobre esa información. Pero también es cierto que esas leyes resultan insuficientes para una efectiva protección de los usuarios y su privacidad. En primer lugar porque son leyes limitadas al aviso por parte de las empresas que sus datos están siendo utilizados. En segundo lugar porque estas leyes pueden no ser seguidas por Google en la medida en que ésta se ampara en una legislación ajena a la del propio usuario, al menos en el contexto europeo. En tercer lugar porque el uso de información personal no documentada atiende a cuestiones técnicas por un lado y de intereses de cibernautas por otro.

Estos hechos sitúan al usuario, de facto, en una situación de desamparo legal respecto al uso y tratamiento de su información personal no documentada. Así la respuesta a la quinta pregunta podría resultar que existe una violación del derecho a la privacidad de los usuarios por parte de Google en la medida en que no existen mecanismos suficientes que lo salvaguarden. Ahora bien, desde la perspectiva de la compañía esta afirmación no es del todo cierta. Google sí que ofrece a sus usuarios herramientas para proteger su privacidad y el uso de datos personales. Éstos pueden, en cierta medida, decidir qué información puede ser utilizada y editar en cualquier momento su privacidad. En este sentido es cierto que Google vela por mantener la privacidad de sus usuarios.

Sin embargo, esta posibilidad de edición de la información resulta limitada cuando se trata de información personal no documentada, aquella que tiene que ver con los datos de navegación de los usuarios y que es el ejemplo utilizado en este momento de la investigación. Éstos pueden limitar ciertas acciones como eliminar los datos relativos a la ubicación de algunos servicios, navegar de forma que no se almacenen los datos de navegación de una sesión concreta, etc. Pero el almacenamiento de esos datos, el rastreo del tráfico generado por el usuario, el uso de determinadas cookies, etc., quedan al margen de lo que éste puede controlar sobre su información. En este sentido, la protección de la privacidad de los usuarios es limitada, y podría decirse nula, si se entiende por privacidad aquella información personal no documentada.

5.9.6. Protección de la información personal no documentada adquirida

La sexta y última pregunta es formulada una vez la invasión de la privacidad se ha llevado a cabo, y tiene que ver con la protección sobre la información una vez se ha conseguido. Según Parent,

> We can say that the right to privacy is violated when the undocumented personal information acquired is not adequately protected against unwarranted cognitive intrusion or unauthorized uses. It is also violated, of course, by actual instances of such intrusions and uses.
> (Parent, 1983, p. 281)

En principio, en la medida en que el usuario es informado de que su información va a ser utilizada y compartida en el ciberespacio no se podría decir que está habiendo un uso inadecuado de la información. En este sentido, la antes mencionada "Ley de cookies", lejos de proteger al usuario, se vuelve contra él en la medida en que le entorpece a la hora de pedir responsabilidades sobre el uso de la información. Como el usuario ya está informado de que se va a rastrear su información personal no documentada y que se va a compartir con terceros (cookies de terceros) pierde toda posibilidad de denunciar el uso de esa información.

La cuestión del control sobre esa información resulta complicada, debido principalmente a la característica ya mencionada de convertirse en información grasienta. Una vez que la información se ha digitalizado o creado y/o introducido en la red, en virtud de la capacidad combinatoria y reproductiva de dicha información, ésta es muy difícil de acotar en un lugar concreto que permita un control efectivo sobre su uso. Cuando un usuario se introduce en un sitio web existen muchos

agentes que tiene acceso a esa información, desde la propia web a otros sitios relacionados con ella, como pueden ser los agentes publicitarios, las redes sociales a las cuales se pueda dirigir el usuario desde el sitio, Google y sus herramientas de tráfico, etc.

Todos estos agentes tienen acceso a información personal no documentada del usuario que pueden compartir con terceros. Imagínese por ejemplo que el sitio web concreto es una web de noticias. En este sitio no sólo están las noticias que publica sino también, varias redes sociales desde las cuales el usuario, si lo desea, puede publicar en su cuenta una noticia en concreto. Estas redes tendrán entonces acceso a la información personal no documentada del usuario. También es probable que este sitio tenga algún tipo de publicidad contratada. Si el usuario clicase sobre un anuncio entonces el anunciante y la empresa que le haya vendido el espacio publicitario, que como se ha visto seguramente será Google, tendrá acceso a la información del usuario. Todas estos actores podrán almacenar, compartir y duplicar esa información tantas veces como quieran, generando así una información grasienta.

Controlar entonces la información contenida en la red resulta complicado de llevar a cabo. En el caso de Google, ya avisa en su Política de privacidad que "cada vez que utilizas nuestros servicios o consultas nuestro contenido, obtenemos y almacenamos determinada información en los registros del servidor de forma automática". Así mismo, como dueña de muchos servicios "podemos combinar información personal de un servicio con otro tipo de información, incluida información personal de otros servicios de Google". Por otra parte, como se decía más arriba cuando se trataba la dificultad de aplicar determinadas leyes, "podremos llevar a cabo el tratamiento de tus datos personales en un servidor que no esté ubicado en tu país de residencia", lo que significa no tenerse que acoger a las leyes del país desde el que se realiza la conexión.

El carácter grasiento de la información es visible también en la Política de privacidad de Google ya que "aunque elimines tus datos de nuestros servicios, es posible que no destruyamos de inmediato las copias residuales almacenadas en nuestros servidores activos ni los datos almacenados en nuestros sistemas de seguridad". Por otra parte Google comparte información de los usuarios con "nuestros afiliados, o a otras personas o empresas de confianza para que lleven a cabo su procesamiento por parte de Google, siguiendo nuestras instrucciones y de conformidad con nuestra Política de privacidad". También puede ser compartida por motivos legales "con empresas,

organizaciones o personas físicas ajenas a Google si consideramos de buena fe que existe una necesidad razonable de acceder a dichos datos o utilizarlos, conservarlos o revelarlos".

Todas estas situaciones en las que se está compartiendo información personal no documentada (y documentada) de los usuarios son notificadas a éstos, y en la medida en que se aceptan las condiciones de uso de los servicios se está aceptando ese tratamiento de la información. Ahora bien, también es cierto que aquello que se acepta es aquello de lo cual el usuario está informado. Podría estar sucediendo que no se esté dando una información completa sobre cómo será utilizada la información o que el usuario no sea capaz de comprender aquello que firma o que simplemente no lea aquello que está firmando. Así mismo, como esa información es compartida con terceros, el usuario puede estar firmando un acuerdo con Google pero no con las terceras partes implicadas en el uso de la información, por lo que la desprotección puede continuar a pesar de estar protegido por su Política de privacidad.

5.9.7 Resumen

Una vez hecho el análisis éste ofrece varias conclusiones relativas a la seguridad de la privacidad de los usuarios de Google. Recuérdese que las preguntas iban encaminadas a saber si la privacidad se infringe de un modo justificado o injustificado. Como apunta el propio Parent, las cuatro primeras preguntas se refieren a la justificación de la invasión de la privacidad, la quinta a la invasión misma y la sexta a la situación que surge una vez ésta ha sido realizada.

Los motivos que se han señalado para una invasión de la privacidad de los usuarios por parte de Google son, por un lado cuestiones técnicas, dentro de las cuales están la mejora de la funcionalidad, la navegabilidad y la experiencia del usuario. Por otro lado, esta invasión de la privacidad es necesaria para que Google y los usuarios-productores obtengan beneficios en el ciberespacio. Podría entenderse que ambos motivos no tienen el mismo peso justificativo y que mientras está justificada la invasión de la privacidad para mejorar los servicios de los usuarios no lo está tanto para que las empresas, incluida Google, obtengan beneficios. Pero, antes de adoptar esta postura, es necesario tener en cuenta ciertos aspectos.

El primero de todos es algo que ya se ha ido mencionando a lo largo de esta investigación y tiene que ver con que Google es una empresa privada con el objetivo claro de generar beneficios. La forma en que esto se consigue es, actualmente, mediante la gestión y venta de información personal

no documentada. Los servicios que ofrece a sus usuarios tienen como coste el acceso a ese tipo de información, hecho que por otra parte no se les oculta. En segundo lugar es importante entender que los usuarios-productores suponen una parte fundamental del ciberespacio y que éstos también deben tenerse en cuenta a la hora de reflexionar sobre los motivos y la justificación de la invasión de la privacidad.

El comercio electrónico es una parte fundamental tanto del ciberespacio como de la economía en general. Una de sus características fundamentales es la capacidad de llegar a un público amplio y objetivo y esto se consigue a través del conocimiento sobre el comportamiento de los usuarios-compradores, que viene determinado por el uso de información personal no documentada.Los estudios de mercado, el análisis de datos o la grabación en circuitos cerrados de vídeovigilancia son prácticas habituales en la mayoría de establecimientos, situaciones en las que los compradores no sienten que su privacidad está siendo invadida. Habría que entender desde esta perspectiva el uso de información personal no documentada por parte de las empresas en línea.

A la hora de interpretar la legitimidad y la importancia de la privacidad se veía cómo tanto para Google como para los usuarios-productores, el uso de este tipo de información era legítimo e importante ya que ésta supone su mayor y más fiable fuente de ingresos. Para los usuarios-consumidores esta legitimidad e importancia estaba relacionada con el mantenimiento de unos servicios gratuitos, que podía ser suficiente para legitimizar ese uso. La importancia vendría determinada por el interés de obtener cierto tipo de ciberespacio personalizado.

Cuando se ha cuestionado la importancia del conocimiento adquirido a través de esa intromisión en la privacidad se ha visto que Google defiende un almacenamiento de la información de forma anónima. La importancia del conocimiento estriba en poder ofrecer a todos sus usuarios los productos más adecuados a cada uno de ellos. El objetivo de Google no es tener un conocimiento individualizado de las personas sino patrones de conducta de unos usuarios para vender esa información, en forma de estadísticas a otros. Sin embargo se ha señalado también que el modo en que se cosecha, almacena, distribuye y recombina la información del ciberespacio es, en cualquier caso, una situación abusiva para los usuarios-consumidores.

Este hecho, se había señalado, no se limita sólo a Google. El problema del uso y gestión de la información personal no documentada es un problema general de las tecnologías digitales. Es

necesario delimitar los objetivos por los que esa información se almacena, construir mecanismos que permitan a los usuarios cierto control sobre la gestión de esa información, marcar una caducidad sobre su almacenamiento, crear mecanismos que limiten su transferencia, etc. Habrá que hacer todo esto, sin embargo, teniendo en cuenta que se estarán cambiando las bases que ayudaron a crear el ciberespacio ahora conocido, unos cimientos basados en la cultura libertaria de la comunicación del conocimiento y de la información. Una vez construido es difícil ver el peligro que puede albergar limitar el modo en que se mueve la información que no deja de ser conocimiento. Si al construir este espacio social se hubieran impuesto restricciones a este movimiento, el ciberespacio sería un lugar diferente, mejor o peor es tema para la especulación. Sin embargo hay que tener en cuenta las posibles consecuencias a la hora de limitar la circulación de la información.

En cuanto a las alternativas para la adquisición del conocimiento se ha visto que, debido a la naturaleza de la propia información, no existen alternativas para alcanzar ese conocimiento. En la medida en que se ha definido esa información personal no documentada para este análisis como tráfico generado por un usuario en la red, no sería posible acceder a ese conocimiento si no es a través del rastreo de ese movimiento del usuario por el ciberespacio.

En cuanto a las restricciones sobre el uso de esa información una vez se ha adquirido se ha señalado la legislación existente a este respecto. Se ha dicho que esas leyes, como la Ley de cookies, no son suficientes para proteger la privacidad de los usuarios. De hecho, en cierta medida, esas leyes suponen una desprotección ante el uso indiscriminado de la información. El hecho que el usuario sea informado sobre el uso de cookies que permiten el rastreo de su movimiento por la red, y que éste podrá ser compartido con terceros, no implica que su privacidad se vea protegida. Sin embargo, permite a los usuarios-productores evitar cualquier tipo de denuncia al respecto. Con este tipo de leyes lo que se consigue es la protección de aquellos usuarios que hacen uso de la información personal no documentada de los usuarios-compradores y la desprotección de éstos.

En resumen podría decirse que esta prueba sobre la justificación o no de la invasión de la privacidad no obtiene resultados concluyentes, en la medida en que no puede afirmarse o negarse la justicia de esa invasión. Sin embargo, sí que se desprende de este análisis ciertos aspectos de esta invasión. En primer lugar deja clara la distinción entre ambos grupos de usuarios, con unos intereses contrapuestos para cada uno de ellos. Los usuarios-productores necesitan acceso a la información personal no documentada de los usuarios-compradores, o dicho de otro modo, la no privacidad de

unos es el beneficio de otros. Mientras unos crean productos a base de este tipo de información los otros reciben esos productos basados en los intereses que se desprenden de esa información. En segundo lugar que, de haber invasión de la privacidad por parte de Google, ésta se hace de modo generalizado en el ciberespacio, en tanto mecanismo de producción de beneficios y base de la economía digital. Ya se ha hecho notar que la generalización no significa que la práctica sea correcta. Pero, al someter a prueba a una compañía en concreto, en este caso Google, se observa que ésta mantiene ciertas medidas de protección de la privacidad de sus usuarios, más allá incluso, en algunos casos, de las impuestas por la ley.

Resulta importante señalar que este análisis parte de un concepto de privacidad determinado. Éste entiende que la información generada por un cibernauta cuando navega por la red tiene carácter de privado. Esta interpretación se ha mantenido en este ejemplo en la medida en que la ciberética y su planteamiento actual así lo entienden. Era necesario, entonces, si se pretendía realizar un análisis del modo en que la ciberética interpreta la privacidad. Sin embargo, desde el punto de vista aquí defendido, habría que analizar la idoneidad de ese planteamiento y de no encontrarse razones suficientes para que sea considerada de ese modo contemplar la posibilidad de excluir del ámbito de la privacidad tal información. Este es el objetivo del siguiente capítulo, donde se analizará la adecuación del concepto de privacidad existente y donde se elaborará una propuesta de privacidad digital.

CAPÍTULO 6:
PRIVACIDAD ANALÓGICA Y PRIVACIDAD DIGITAL

6.1. Privacidad analógica

A lo largo de esta investigación se ha hablado de la importancia de la privacidad en el ciberespacio e Internet. Se han analizado las diversas posturas ciberéticas respecto a cómo se entiende la privacidad y cómo la entiende Google. Además, se ha ido advirtiendo de las dificultes que atañen a una concepción de la privacidad que se ha denominado aquí privacidad analógica. Sin embargo, aunque del propio análisis aquí mostrado se desprende qué se entiende por privacidad analógica y cuáles son los problemas aquí aducidos, es conveniente presentar de forma separada este concepto y sus inconvenientes.

En primer lugar se podría decir que la privacidad analógica es aquella constitutiva del, denominado por Echeverría, segundo entorno. Recuérdese que éste era aquel entorno que ya no era el natural, sino el social y cultural. La forma que adoptaba no era la naturaleza, como en el primer entorno, sino los pueblos y ciudades. En este entorno se constituyen además diversas formas sociales como la vestimenta, la familia, la persona, el mercado, la empresa, la industria, el dinero, las escuelas, la ciencia, las máquinas, etc. Aparecen, así mismo, diferentes formas de poder: el militar, el religioso, el político o el económico.

Es en este contexto social y cultural donde la privacidad analógica toma forma, como una expresión más de ese carácter social y cultural del segundo entorno. Esto no significa que en primer entorno no hubiera privacidad, sino que es en este entorno donde adquiere los atributos que más tarde serán inconvenientes para habitar el tercer entorno. "Sobrevivir en E2 (segundo entorno) plantea grandes dificultades para cada individuo, y no digamos alcanzar cierto nivel de bienestar. Para lograrlo hay que desarrollar gran cantidad de técnicas y habilidades*"* (Echeverría, 1999, p. 44). Esas dificultades que conlleva habitar el segundo entorno, así como la aparición de formas sociales basadas en el esfuerzo personal junto con los diversos poderes antes mencionados, llevan a los seres humanos, ahora ya individuos y ciudadanos, a establecer barreras y separaciones entre aquello propio y aquello colectivo, entre aquello que les hace individuos y aquello que les constituye como pueblo, entre aquello conseguido y aquello dado, aquello púdico y aquello impúdico.

La forma social de la vestimenta junto con el poder religioso determinan que el cuerpo deba ser protegido con privacidad. El cuerpo se vuelve algo pecaminoso y es necesario apartarlo del resto de individuos a través de una vestimenta adecuada. Como herramienta de trabajo, debe ser también protegido adaptando la ropa a la situación que se esté desarrollando en el segundo entorno. La

familia es también objeto de la privacidad. En ella, distinguiéndose del pueblo, del lugar de trabajo o de la iglesia, se desarrollan relaciones diferentes a las del resto de individuos y grupos del segundo entorno. La casa, espacio donde convive la familia, es también un espacio privado, en la medida en que es en ella donde ser lleva a cabo esa relación familiar. Las formas sociales del trabajo, la empresa y el dinero refuerzan la idea de propiedad privada. Las relaciones sociales entre individuos se jerarquizan: dios, la familia, los vecinos, el trabajo, el poder político, etc. Entre ellas media el grado de privacidad implicado.

Como constructo social, debe decirse que la privacidad es artificial. Aunque ligada a la naturaleza y por lo tanto al primer entorno, el cuerpo forma de la naturaleza y por lo tanto está asociado a aquél, la privacidad no es necesaria en ese entorno. No hay nada en la naturaleza que la determine. Por lo tanto, como mecanismo artificial, debe ser susceptible de ser construida de nuevo. En esta investigación se han señalado tres inconvenientes fundamentales de esta privacidad del segundo entorno que dificultan su adecuación para el ciberespacio o tercer entorno. Se ha dicho que es una privacidad que mantiene la separación entre los espacios público y privado; que está descontextualizada del lugar donde se desarrolla y; que no tiene en cuenta las propias decisiones de los individuos a la hora de proteger su privacidad.

La primera dificultad a la que se enfrente la privacidad analógica tiene que ver con el mantenimiento de dos esferas o espacios separados, el público y el privado. Cuando se ha tratado el punto de vista de Helen Nissenbaum ya se ha visto cómo esta dicotomía es considerada por la autora como un problema conceptual que, además de ser sostenido por los estudiosos de la ética en el ciberespacio, impide generar un debate en torno a la privacidad en público. Esta separación es mantenida de forma artificial, basada en supuestos anteriores al tercer entorno y creados para mantener la distancia entre formas sociales diversas. Así, se veía cómo aquello perteneciente al ámbito privado tenía que ver con la familia, con los trabajadores, los ciudadanos, etc., en contraposición a aquello público relacionado con el civismo, la empresa o el gobierno. Dicho de otro modo, mientras la privacidad pertenece al reino de los individuos, lo público pertenece al de las representaciones sociales de ellos.

Si bien Nissenbaum denuncia esta dicotomía para afirmar la necesidad de poder hablar de una privacidad en público en el contexto de esta investigación se remarca la disolución de estos ámbitos o al menos su difusión. Sencillamente, la forma actual de entrar en el ciberespacio, el modo en que

se habita y los diferentes usos que los cibernautas le dan, no distingue ambos entornos como separados. En todo momento se está en el ciberespacio. Los individuos mantienen siempre un canal abierto a él, con independencia del lugar físico donde se encuentren. Las nuevas formas de relaciones sociales, de trabajo, de ocio, de adquisición de productos, no distinguen entre aquello que se tenía como privado y lo que se tenía como público. Aquellos ámbitos que tradicionalmente se tenían como en esferas separadas, el cuerpo, la familia, las relaciones interpersonales, cada vez más se desplazan hacia ese tercer entorno. Las relaciones amorosas y sexuales se producen en este entorno, las familias permanecen unidas o se disgregan también en él, el cuerpo se muestra y se transforma en función de las tendencias que se den en el tercer entorno, etc.

Las tecnologías digitales han supuesto también que el espacio público se transforme en espacio privado y a la inversa. Las acciones que se llevaban a cabo en cada uno de estos ámbitos separados han visto cómo esas barreras sociales y psicológicas han caído y lo que se mantenía en la esfera de lo privado ahora se puede hacer en público y aquello público se puede realizar donde antes sólo lo privado.

Podría parecer que la privacidad ha perdido terreno frente a lo público y el hecho de permanecer siempre en el ciberespacio dificulta el mantener espacios para la reclusión, la soledad y el anonimato del que hablaba Ruth Gavison. Pero hay que tener en cuenta que lo privado ha ampliado su terreno hasta alcanzar la esfera de lo público. La posibilidad de realizar situaciones privadas en público es una novedad del tercer entorno y del ciberespacio y es en este sentido donde la privacidad debe tenerse como beneficiaria.

La cuestión radica, para ambas esferas, en que éstas han sufrido una transformación que debe ser asimilada. Hay que ser conscientes, y actuar y pensar en consecuencia, del cambio de paradigma social. El ciberespacio o Internet no se tratan tan sólo de una nueva invención tecnológica que haya venido a facilitar las comunicaciones, se tratan más bien de una nueva forma de estar y habitar el mundo. Como tal, deben darse también novedades en el modo en que se entienden esas formas sociales construidas, entre ellas, el concepto mismo de privacidad. De ahí la necesidad de una privacidad digital, de una teleprivacidad utilizando el vocabulario de Echeverría, o una ciberprivacidad en el contexto de esta investigación.

Como segundo inconveniente de la privacidad analógica se ha dicho que está descontextualizada del lugar donde se desarrolla. Esta segunda dificultad viene determinada por la primera ya que, al entender que en ciberespacio se mantienen las esferas de lo público y lo privado, se da por hecho que la privacidad debe mantener también la misma forma que en el segundo entorno. Pero lo cierto es que el modelo de Internet que se ha visto, dejando de lado la web profunda donde sí se mantendría hasta cierto punto las esferas separadas, no está construida para que la privacidad permanezca como se entendía en el segundo entorno.

Se ha visto cómo la personalización de contenidos, la experiencia del usuario, el rastreo y análisis del tráfico web o la capacidad de almacenamiento, son partes inherentes a este entorno. El funcionamiento de la red, tal y como es ahora, parte de la necesidad de todos elementos. En la medida en que alguno disminuya su eficacia lo hará también la red misma. Dicho de otro modo, no es posible una Internet a medida de cada uno de los usuarios si no se pueden obtener sus datos. Esta es una cuestión técnica. Del mismo modo que no es posible que un vendedor sepa lo que se quiere comprar si no se le dice aquello que se está buscando, la red no puede ofrecer resultados si no se le informa sobre la búsqueda.

Es importante además, partiendo del ejemplo dado, Google, que no es posible el uso de los servicios y herramientas que ofrece la compañía si ésta no puede acceder a los datos de los usuarios. No es posible ofrecer una buena ruta para ir de un lugar a otro sin conocer la posición actual, no es posible ofrecer resultados de búsqueda en el idioma del usuario si se desconoce cuál es ese idioma, no es posible realizar una compra en un sitio web si no se permite la inclusión de las herramientas que permitan navegar de una página web a otra sin que se pierdan los productos seleccionados y no es posible ofrecer el mismo periódico digital cada vez que se busquen noticias si no se deja al navegador memorizar cuál es ese periódico favorito.

En otras palabras, no es posible mantener la estructura del ciberespacio y de Internet si toda la información de los usuarios contenida en él tiene carácter de privada. Es una cuestión de adecuación contextual. Es necesario pensar otro modelo de privacidad que no vuelva poco éticas o antiéticas todas las acciones que se llevan a cabo en el ciberespacio e Internet, ya que en mayor o menor medida, actualmente, siempre se está haciendo uso de información que para alguien puede ser tenida como privada. Podría ser suficiente atender a las *situaciones* propuestas por Moor y Tavani, pero entonces habría que definir en qué situaciones utilizar qué información estará

moralmente permitido. En este caso se corre el riesgo de no atender a cuestiones prácticas y dejarse llevar por el subjetivismo, donde un cibernauta, por ejemplo, por el hecho de ser un usuario-comprador y no uno productor, pueda hacer uso de la privacidad de otro, pero no así una corporación o empresa. El usuario podría estar a favor de esta situación y se estaría efectivamente atendiendo a una situación concreta, pero distaría de ser una situación justa. En primer lugar porque la persona a la cual se refiere esa información podría seguir considerando que se viola su privacidad. En segundo lugar porque se estaría negando a una empresa constructora de ese tercer entorno un beneficio que podría considerar merecer en la medida en que permite y facilita a los usuarios habitar el tercer entorno.

Por último se ha hablado de la privacidad analógica como ajena a las propias decisiones de los cibernautas a la hora de proteger su privacidad. Este inconveniente tal vez sea el más difícil de justificar, ya que no es posible, en el contexto de esta investigación, demostrar empíricamente en qué medida los cibernautas aseguran su privacidad. Haría falta un estudio de campo y longitudinal sobre esta cuestión para confirmar esta afirmación. Sin embargo, hay un hecho fundamental que posibilita confirmar en cierta medida esta postura. Es la existencia de la web profunda, donde efectivamente no existe un rastreo del tráfico web, una personalización de contenidos ni un uso de información de los usuarios. Sin embargo, una mayoría de cibernautas continúan usando la web superficial. Si entendieran la privacidad como un elemento importante de la navegación por el ciberespacio, entonces utilizarían la web profunda para hacerlo. No existe ninguna traba para que navegan por esta red, nada les impide habitar el ciberespacio de forma anónima, secreta y solitaria. El único impedimento que pueden encontrar es no querer hacerlo. Y uno de los motivos por los que pueden no querer hacerlo es porque deseen permanecer en las redes sociales como las conocen, que la personalización les muestre los resultados que según el modelo de usuario predice les interesen y que el tráfico que generan no les suponga ningún inconveniente para todo ello.

La propuesta de Marc Prensky de distinguir entre nativos digitales e inmigrantes digitales resulta, en estos momentos, adecuada. En su exposición la cuestión fundamental estriba en el modelo educativo que se ha de seguir a la hora de enseñar a los nativos digitales pero el punto de partida sitúa la discusión de esta última dificultad de la privacidad analógica en un contexto determinado.

> So what does that make the rest of us? Those of us who were not born into the digital world but have, at some later point in our lives, become fascinated by and adopted

> many or most aspects of the new technology are, and always will be compared to them, Digital Immigrants. The importance of the distinction is this: As Digital Immigrants learn – like all immigrants, some better than others – to adapt to their environment, they always retain, to some degree, their "accent", that is, their foot in the past. (Prensky, 2001, pp. 1-2)

Ese acento o mirada hacia el pasado de los inmigrantes digitales es importante a la hora de hablar de la privacidad en el ciberespacio e Internet. La construcción de éstos ha sido llevada a cabo por esos inmigrantes, que han tenido que mirar atrás a lo ya conocido para crear esas estructuras nuevas. Se han tomado las referencias del segundo entorno y se han querido instalar en este tercer entorno. No se ha cuestionado que las formas que valían en aquél pudieran valer en éste. Se ha trasladado una noción de privacidad de un lugar a otro sin tener en cuenta su adecuación. No sólo los constructores sino la propia filosofía y ética, volviendo así a la crítica de Nissenbaum, han mantenido un concepto de privacidad tradicional que no les permite encontrar soluciones a las dificultades de proteger la privacidad en el ciberespacio.

> But this is not just a joke. It's very serious, because the single biggest problem facing education today is that our Digital Immigrant instructors, who speak an outdated language (that of the pre-digital age), are struggling to teach a population that speaks an entirely new language. This is obvious to the Digital Natives – school often feels pretty much as if weve brought in a population of heavily accented, unintelligible foreigners to lecture them. They often can't understand.
> (Prensky, 2001, p. 2)

La privacidad, como la educación de la que habla Prensky, debe explicarse y entenderse desde ese nuevo lenguaje, un lenguaje digital donde cabe la posibilidad que todo aquello que los inmigrantes digitales entienden por privado no sea comprensible para los nativos, donde la información personal, por ejemplo, no sea relevante. Es necesario escuchar y aprender cómo se dice privacidad en el lenguaje digital, qué sentido tiene y cuales son los elementos de los cuales participa. En definitiva, de lo que se está hablando es de la necesidad de alcanzar un horizonte de sentido.

Todas las formas sociales han sufrido transformaciones debido al impacto de las tecnologías digitales y el ciberespacio. La biotecnología, el arte digital, las relaciones sociales digitales, el

aprendizaje electrónico, el comercio electrónico, el teletrabajo, las comunicaciones electrónicas, etc., son adaptaciones de las formas sociales del segundo entorno a este digital. La filosofía y las cuestiones que trata deben también amoldarse a este espacio. Amoldarse no significa aquí perder su forma para poder encajar. Significa tener la capacidad de adaptación, encontrar un lugar donde sea posible seguir desarrollándose plenamente, buscar un sitio que sea adecuado para su despliegue. Del mismo modo que los inmigrantes digitales tienen que aprender el nuevo idioma para poder entrar en comunicación con los nativos digitales, la filosofía debe aprender a hablar ese lenguaje, un nexo comunicativo que le permita expresar sus ideas y que éstas lleguen al interlocutor. De ahí la necesidad de pensar la privacidad desde el lenguaje digital.

6.2. Privacidad digital

Se ha dicho en esta investigación que el ciberespacio es eminentemente informacional. Recuérdese que Echeverría proponía como cuarta propiedad del tercer entorno ese carácter informacional, frente a la materialidad del primero y el segundo. "El tercer entorno es informacional y, como veremos más adelante, digital, porque los bits de información, y no los átomos, son los que permiten conformar las diversas representaciones que componen E3*"* (Echeverría, 1999, p. 70). Por su parte, Manuel Castells proponía como nuevo paradigma tecnológico del siglo XXI el informacionalismo (Castells, 2006, p. 33). Este sistema de información, afirma, tiene tres características esenciales que le hacen diferencia de los sistemas anteriores: "su capacidad auto-expansiva de procesamiento y de comunicación en términos de volumen, complejidad y velocidad; su capacidad para recombinar basada en la digitalización y en la comunicación recurrente; su flexibilidad de distribución mediante redes interactivas y digitalizadas" (Castells, 2006, p. 34).

Se ha visto también cómo las primeras preocupaciones de la ciberética iban encaminadas en dirección hacia la privacidad y estaban relacionadas con el tratamiento que se daba a esa información, que podía considerarse privada. Las propuestas, se han visto, eran entender la privacidad como control, acceso, con determinado valor, etc., de esa información contenida en el ciberespacio. Es razonable entonces, afirmar que la primera característica de la privacidad digital es su carácter informacional.

Es cierto que la privacidad analógica tiene algo de informacionalidad, en la medida en que el desocultamiento de determinada información tiene que ver con la pérdida o no de privacidad. Pero, en virtud de su presencia en el segundo entorno, donde prima la materialidad frente a la información

y donde existe una clara separación entre las esferas públicas y privadas, en la privacidad analógica se tiende hacia la materialidad de la privacidad. Así, una pérdida de privacidad es entendida como el acceso a un terreno particular o privado de las personas, el acceso a su casa, el acceso a su cuerpo, el acceso a sus posesiones, etc. Sin embargo, en la privacidad digital, en la medida en que la materialidad carece de importancia ya que las cosas físicas no tienen presencia en el ciberespacio, la privacidad debe entenderse esencialmente como informacional.

Siendo una privacidad informacional y exclusiva de las tecnologías digitales, el ciberespacio e Internet, en la medida en que es una teleprivacidad que se desarrolla en Telépolis, pierde la distinción entre los espacios público y lo privado, al menos en el sentido tradicional.

> El nombre de "Telépolis" viene a marcar la oposición entre las formas clásicas de organización social [...] Su estructura topológica básica no es el recinto con interior, frontera y exterior, sino la red de interconexiones que vincula puntos geográficamente dispersos, pero unidos por la tecnología.
> (Echeverría, 1999, p. 160)

Como ciudad, en Telépolis o el ciberespacio las relaciones humanas se desarrollan en espacios públicos. Las interacciones en el segundo entorno se llevaban a cabo en la plaza, el mercado, los lugares de ocio, los centros de estudio, etc. Como afirma Tavani (2005), hubiera sido impensable, en estos lugares del segundo entorno, exigir a las autoridades que mantuvieran la privacidad de los ciudadanos que participaban en estos espacios públicos, precisamente por su carácter de espacio público. Lo mismo sucede en el tercer entorno. Como espacio eminentemente público no es posible hablar de privacidad en él, en la medida en que no hay cabida para hablar de privacidad en espacios acotados.

Recuérdese el ejemplo que ponía Moor de la situación en la que un individuo se encontrara en lo alto de una montaña, disfrutando de privacidad pero que, en un momento dado, perdiera esa privacidad porque alguien más ha subido a la cima y le ha visto. Afirmaba que, en este caso, no ha habido una violación de la privacidad sino una pérdida. Desde el punto de vista aquí expuesto, ni siquiera ha habido una pérdida de privacidad porque nunca la ha habido. El hecho de estar en solitario, sin nadie más, en la cima de una montaña no significa que se esté en una situación privada. Tan sólo afirma la no presencia de otras personas en ese momento dado. Pero se continúa

en un espacio público y abierto. Del mismo modo que si se está paseando por la playa al amanecer y al remontar una duna aparece un grupo de gente en la playa no significa la pérdida de privacidad ya que, como espacio público, la playa nunca ha brindado la posibilidad de que la hubiera. Los espacios públicos, en tanto espacios compartidos, nunca pueden tener el carácter de privados, tan sólo permiten al individuo experimentar la ficción de estar en una situación privada.

El ciberespacio, Telépolis e Internet son espacios públicos, y como tales, no permiten la posibilidad de albergar privacidad. Los movimientos en la red, como el paseo por la playa o el senderismo por la montaña, no deberían entenderse como acciones dotadas de privacidad, sino como situaciones llevadas a cabo en espacios públicos y por lo tanto susceptibles de ser observadas. De este modo, la privacidad digital debe alejarse de aquella información que se desprende de las acciones públicas, ya que de otro modo no se distinguirá de una privacidad analógica, inadecuada para este espacio social que es el tercer entorno. Por otra parte, manteniendo la privacidad dentro de las acciones públicas realizadas en el ciberespacio, no se resolverá el problema de mantener el carácter abierto de la red sin vulnerar de algún modo la privacidad. Ésta debe atender a un tipo de información que sea factible proteger en el ciberespacio.

Dicho esto, surge la pregunta sobre qué debe entenderse por privacidad digital o cuál es su alcance. Aquí se propone una privacidad de mínimos para el ciberespacio. El acceso o el control sobre la información son inadecuados en este entorno. El carácter grasiento de la información se ha visto, por un lado inherente a la información digital y, por otro lado, imposible de minimizar a efectos prácticos. El acceso restringido y controlado sólo añade a la primera propuesta la cantidad de agentes que podrán tener acceso a la información. Pero de nuevo, la *grasiedad* de la información dificulta esa restricción. La privacidad como conocimiento de información personal no documentada suponía que, como se afirma aquí, la información contenida en el ciberespacio, como información documentada tiene carácter de pública.

Desde la perspectiva aquí planteada, la privacidad digital tiene como objeto a salvaguardar sólo aquella información digital privada. Por información digital privada se debe entender aquella información que no es lanzada o dejada en el ciberespacio y que tiene como función principal permitir al ciberciudadano acceder y gestionar en él determinadas acciones. Unas explicaciones son necesarias para entender este concepto de información digital privada.

Las contraseñas de acceso a determinados espacios de Internet forman parte de esta información digital privada. La clave para acceder a las cuentas de correo electrónico, a los perfiles de las redes sociales, a las cuentas bancarias, etc., forman parte de este tipo de información privada. Es información que no pretende almacenarse y *colgarse* en la red. Su finalidad es más bien la de acceso al ciberespacio y a las acciones que se puedan llevar en él. Claro está que pueden almacenarse en los navegadores para su posterior uso y que en ese sentido podrían entenderse como dejadas en la red. Pero no forman parte de este. Es, se podría decir, la llave que permite acceder de un lugar a otro del ciberespacio, pero no es parte de él. Del mismo modo que una llave puede considerarse parte de la cerradura y, en cierta manera, parte del lugar u objeto que abre, pero no identificarse con ninguno de estos elementos, las contraseñas en este sentido tampoco forman parte del ciberespacio aunque se relacionen con él y en algún momento entren en contacto. Este tipo de información debe ser considerada y protegida por la privacidad de los usuarios. No debería tenerse acceso por parte de terceros y su gestión, almacenamiento y duplicación deberían ser respetados en virtud de su carácter privado.

Otro tipo de información digital privada es aquella que puede definirse como documentación digital privada. En esta categoría entrarían, por ejemplo, los correos electrónicos, la mensajería instantánea o los archivos almacenados en los servidores. Cuando se deja un documento en la nube se pretende que el servidor funcione como almacén de esa información. No es información, puede decirse, que navegue por Internet, ni su paso por el ciberespacio pretenda incluirse en él. Esta información es ajena a este espacio y debería entenderse que lo sobrevuela para ir a almacenarse al lugar de destino. En este sentido, la nube debe entenderse como una herramienta de almacenamiento y no como parte de Internet y por ende como espacio compartido.

El correo electrónico y la mensajería instantánea son otro tipo de información digital privada. Ambos tipos de comunicaciones utilizan el ciberespacio como medio para llevar a cabo tal acción comunicativa. El contenido de la conversación o el mensaje tampoco debe formar parte del ciberespacio, aunque se utilice como medio. No es información dirigida a utilizarse ni dejarse en la red, sino un tipo de información que se envía de un(os) destinatario(s) a otro(s). Su uso, almacenamiento y gestión más allá del necesario para alcanzar el acto comunicativo entre ambos extremos es una pérdida y su uso para otro fin es una violación de la privacidad digital.

Por último, existe otro tipo de información digital privada que tiene que ver con aquella confidencial. En este sentido podría decirse que es una información digital confidencial. Ésta está relacionada con aquella información que, normativamente, no debe ser compartida en la red, como los datos bancarios o los informes médicos. Este tipo de datos son digitales en virtud de haber sido digitalizados para su mejor gestión, pero no deben tenerse como digitales propiamente dichos. Su formato es accidentalmente digital pero su interés no es el tercer entorno sino el segundo, donde la materialidad todavía tiene cabida. Es información relativa al cuerpo y al dinero de los cibernautas.

Su interés es ajeno al ciberespacio y éste sólo es, otra vez, el medio por el cual se presenta la información. Así mismo, son datos que pueden considerarse como sensibles ya que su conocimiento público puede influir de forma negativa en la vida de las personas. El caso de los datos bancarios tiene una importancia normativa, en la medida en que en la cultura occidental se considera inapropiado conocer la solvencia económica de las personas, aunque se exija de las personas públicas saber esta situación. Por su parte, los datos médicos tienen un carácter especial. Estos, podría decirse, son el único tipo de información que podría considerarse genuinamente privada, ya que se refiere al cuerpo de cada individuo. El conocimiento por parte de personal sanitario de esta información resulta inevitable, pero su respeto y confidencialidad están asegurados por varios mecanismos, tanto normativos como morales o éticos.

Tanto los datos bancarios como los médicos deben ser tenidos como pertenecientes al ámbito de la privacidad digital. Su uso, almacenamiento y dispersión sin el consentimiento explícito e informado de los particulares debe ser eliminado y cualquier vulneración respecto a su confidencialidad juzgada y condenada.

Dicho esto, aquella información digital que no forme parte de las categorías antes mencionadas no debería considerarse, desde el punto de vista aquí esgrimido, como información privada. El hecho que pueda ser almacenada, distribuida y gestionada sin precedentes históricos, esto es, la pérdida de control sobre mucha información lleva a los usuarios, a los teóricos y a las instituciones a creerse en la necesidad de marcar límites al uso de información. Pero visto con perspectiva, resulta irrelevante para la privacidad de los individuos que sus movimientos en la red sean registrados y almacenados o que sus perfiles en las redes sociales, ya por definición públicos, sean utilizados por terceros para ofrecerles publicidad. La privacidad de los cibernautas debe centrarse en la información verdaderamente relevante para su privacidad, y ésta es la relacionada con su documentación

personal, su información confidencial y las herramientas de las que dispone para acceder al ciberespacio.

Con esta privacidad digital se mantiene la privacidad de los individuos, se permite a los usuarios-productores seguir construyendo el ciberespacio que los propios cibernautas demandan y se resuelven problemas que plantea la ciberética. No es una cuestión de accesibilidad, de control, de diferenciar espacios o de distinguir entre información documentada o no documentada para proteger la privacidad. La privacidad digital es una combinación de todas ellas, que como Google, pretende tomar lo mejor de sus predecesoras para fortalecer y emprender el camino hacia un mejor y más seguro ciberespacio.

CAPÍTULO 7:
CONCLUSIONES

Al comienzo de esta investigación se han planteado varias cuestiones relativas a la situación de la privacidad por el uso de las tecnologías digitales y en concreto de la privacidad en el ciberespacio e Internet. Se ha comenzado afirmando la migración masiva hacia ese espacio digital donde los seres humanos desarrollan, cada vez, las formas sociales que le ayudan a habitar el mundo. Como espacio de interacción humana es importante que todas las ciencias, sobre todo las involucradas en preservar y mejorar esa comunicación, sean partícipes de la construcción de los medios y mecanismos donde ésta pueda darse de un modo adecuado para todos los agentes involucrados. De ahí la importancia de una filosofía y una ética que continúen articulando un discurso racional para resolver las preguntas que puedan surgir en este nuevo espacio.

Uno de los hechos que se querían mostrar era que el ciberespacio es primeramente un espacio informacional y que todo aquello que en él sucede tiene carácter informativo. Con Manuel Castells y Javier Echeverría se ha visto que las tecnologías digitales han supuesto para la sociedad un cambio de paradigma que puede denominarse informacionalismo. Éste, se ha visto, es un paradigma tecnológico basado en un modo revolucionario de producir y gestionar la información, con un gran impacto en el conocimiento. Recuérdese que se ha dicho que todas las sociedades anteriores han tenido sus avances y su evolución en el conocimiento, de ahí que el uso del término "sociedad del conocimiento" no sea del todo adecuada para hablar de la sociedad de las tecnologías digitales. Por ello, se había convenido, junto a Castells, de hablar de sociedad red.

Esta sociedad red, que habita en Telépolis, la ciudad del tercer entorno, se basa en una estructura social constituida por redes de información. Esto significa que todas las formas sociales que adoptan los seres humanos que habitan Telépolis, los telepolitas, ya sean relaciones de producción, de consumo o de poder, se sustentan sobre flujos de información. Lo que caracteriza el nuevo paradigma que posibilita la constitución de esa sociedad red es su flexibilidad, su adaptabilidad y la capacidad combinatoria. Por lo tanto, se ha de decir que las formas sociales de la sociedad red se basan también en esos tres fundamentos. Éstas deben ser capaces de acomodarse, adaptarse y combinarse de modo que puedan desarrollarse en este espacio informacional. Una de las preguntas de investigación planteadas en este estudio era observar el modo en que la tecnología, la filosofía y los seres humanos habían migrado hacia ese entorno. En qué medida han sido capaces de adoptar la flexibilidad, el modo en que se han adaptado y se adaptan a este medio y de qué formas se combinan entre sí para lograr un entorno social que sea beneficioso para todos ellos.

Precisamente se planteaba como problema la existencia de una fragmentación entre estos tres agentes involucrados. Ruptura que se pretendía mostrar al tratar el tema de la privacidad desde la perspectiva de cada uno de ellos. Se ha visto que la tecnología, la filosofía y los usuarios han asimilado las tecnologías digitales y la migración hacia el ciberespacio a ritmos desiguales y que esto dificulta la comunicación entre las partes. Podría decirse, que la sociedad red de la que participan los tres agentes carece ella misma de aquello en lo que está basada, la conexión entre nodos.

La tecnología, como gran beneficiaria de este entorno digital, se mueve a un ritmo que dificulta que tanto la filosofía como los usuarios sigan su paso. Involucrada de tal modo en sus objetivos, no es capaz de observar con perspectiva lo que conlleva un avance tan rápido de sus propias invenciones, determina sin atender al resto de agentes el modo en que debe hacerse uso de los dispositivos y herramientas que construye. La necesidad de avanzar hacia nuevas y mejores creaciones le lleva a carecer de un análisis global de las consecuencias de las mismas. Su objetivo no es otro que el de seguir hacia adelante sin atender a que ni la filosofía ni los usuarios son capaces de asimilar su velocidad.

De este modo, la filosofía y los usuarios, en la medida en que no se les tiene en cuenta a la hora de hacer evolucionar el espacio que ahora habitan, sienten miedo de no poder controlar aquello que sucede a su alrededor y se ven en una posición de desventaja que les lleva a temer por las creaciones y los avances de la tecnología. Uno de esos temores es la cuestión de la privacidad en el ciberespacio. Siendo éste un medio esencialmente informacional creado y mantenido por la tecnología, en la medida en que los usuarios participan de un modo también informativo, en tanto que su presencia en el ciberespacio es informacional, la privacidad entendida como privacidad de la información es el medio que les permite tener cierta participación sobre lo que les sucede en este espacio. La importancia de la privacidad en la red radica precisamente en ser el único modo en que los telepolitas pueden ejercer presión a los señores del aire que son ahora sus gobernantes.

Se planteaba como problema fundamental de la filosofía a la hora de abordar las cuestiones que plantean las tecnologías digitales respecto a la privacidad, el hecho de no poder despegarse del plano teórico y no ser capaz de crear alternativas prácticas para defender la privacidad en el ciberespacio. Se quería mostrar que este hecho se debe a que la filosofía mantiene un concepto de

privacidad que no encaja con el modelo donde debe desarrollarse y que la aleja de un discurso aplicado.

Se ha mostrado que la filosofía mantiene una idea de privacidad que se ha llamado analógica en contraposición a la concepción de una privacidad digital, aquí defendida. Se había dicho, y se ha probado a lo largo de esta investigación, que la privacidad analógica se basaba en tres supuestos fundamentales que dificultan que a) la tecnología tenga en cuenta el discurso filosófico respecto a la privacidad y, b) que sea capaz de crear un discurso ético aplicado para la defensa de la privacidad en el ciberespacio.

El primer escollo de la privacidad analógica mantenida por la filosofía es permanecer en la dicotomía entre los espacios público y privado. Se ha visto cómo esta forma de privacidad es una versión heredada del segundo entorno. Un entorno no digital donde las diversas formas sociales habían impulsado un concepto de privacidad determinado. La separación entre la vida familiar como espacio privado y la vida social como espacio público venían determinados por la creación de nuevas entidades, el ciudadano, el individuo, la persona. La forma social religiosa imponía mantener la privacidad del cuerpo o la vida familiar alejada de la vista del resto de individuos, de lo público. Así mismo el sistema de producción industrial imponía una separación de espacios, aquello que sucedía dentro de la fábrica y lo que sucedía fuera de ella. Todas estas formas sociales del segundo entorno suponían separar espacios, el individuo, su cuerpo, se movía espacialmente de un lugar a otro. Este movimiento y el cambio de situaciones permitían crear la existencia de espacios separados e inconexos. Las tecnologías digitales han supuesto la disolución de estos espacios. Como se ha visto al tratar las características del tercer entorno que proponía Javier Echeverría, éste no es espacial sino distal y reticular.

Sin embargo, se ha visto cómo todas las teorías propuestas por la ciberética para tratar el tema de la privacidad se basan en la idea de espacios separados donde es necesario suponer un espacio público y otro privado, manteniendo así una privacidad analógica. Incluso Helen Nissenbaum, que propone acabar con la dicotomía entre ambos espacios para avanzar hacia una privacidad en público mantiene la dicotomía. Su propuesta implica la necesidad de incluir dentro del espacio público uno privado pero no la disolución de dos esferas separadas.

Una segunda dificultad de la privacidad analógica era estar descontextualizada del lugar donde se desarrolla. Para mostrar este problema se ha ido viendo a lo largo de esta investigación cómo el ciberespacio es principalmente un espacio informacional, así como abierto y público. Las propuestas teóricas que se han señalado entienden la privacidad en términos de control, acceso, restricción, etc. Pero estas características pierden de vista varios factores que dificultan e incluso impiden hablar de la privacidad en estos términos. Se ha visto que el control sobre la información, en virtud de su capacidad de auto-reproducción, esto es, a su carácter grasiento, es impracticable una vez la información es digitalizada, al menos desde la perspectiva de la red superficial. Por otra parte se ha señalado la imposibilidad de mantener un control total sobre la información producida en el ciberespacio. Así mismo se ha visto cómo es posible la pérdida de control sobre la información pero seguir manteniendo la privacidad. Se ha mostrado cómo el acceso a la información no significaba necesariamente una violación de la privacidad. Incluso en algunos casos, como el propuesto por Anita Allen, el acceso a determinada información suponía proteger o vulnerar la privacidad al mismo tiempo. Por su parte, la privacidad entendida como restricción del acceso a la información mantenía los mismos problemas que las propuestas anteriores. Incluso incluyendo el concepto de situación para determinar ciertos momentos donde la privacidad se pierde o se viola la teoría no permitía llevar a la práctica digital estos argumentos.

Todas estas propuestas se han visto alejadas del contexto donde deben ponerse en práctica. El ciberespacio, ya sea por cuestiones técnicas, empresariales o por decisiones de los propios usuarios, necesita de información para mantenerse. No es posible tratar toda la información contenida en él como privada. Si se continua afirmando que todos los datos del ciberespacio son privados, entonces, en mayor o menor medida, cada actor de la red en algún momento dado estará vulnerando la privacidad de alguien. De ahí la propuesta de una privacidad que de margen al uso de información.

Por último se afirmaba que la privacidad analógica no atiende a las actuaciones de los propios usuarios a la hora de proteger su privacidad. Ésta, recuérdese, se decía que era la más difícil de probar en esta investigación. Para afirmar tal suposición sería necesario un estudio de campo longitudinal que permitiera recoger datos sobre el comportamiento del usuario a la hora de proteger su privacidad. Sin embargo, se ponía algún ejemplo que podían apoyar esta hipótesis. El más fundamental era la existencia de la red profunda, donde los datos de los usuarios permanecen anónimos durante toda la navegación del usuario. Pero la gran mayoría de éstos navega en la red superficial, aquella donde su información permanece al descubierto. Debería entenderse que éstos

prefieren determinadas herramientas y servicios que esta red ofrece, sin importarles el uso de esa información que tanto parece preocupar a la filosofía.

Otro de los objetivos marcados al principio de esta investigación era poner a prueba a una de las empresas productores de Internet frente a las diversas teorías éticas que se mostraban. El ejemplo escogido había sido Google. Como una de las mayores empresas de Internet parecía adecuado tomarla como ejemplo a fin de analizar en qué medida se vulnera o protege la privacidad de los usuarios en la red. Se ha visto como problema fundamental de la empresa la existencia de dos tipos de usuarios, con los que mantiene una relación desigual que le obliga a pivotar entre proteger la privacidad de los usuarios-compradores y ceder parcelas de información de éstos a los usuarios-productores. En un primer momento podría parecer que Google atenta contra la privacidad de sus usuarios, pero una vez sometida a prueba atendiendo a las diversas propuestas teóricas así como a su Política de privacidad, puede afirmarse que la empresa no sólo protege la privacidad de sus usuarios como proponen las teorías sino que no oculta el uso de información de sus usuarios.

Se ha señalado la experiencia del usuario y la personalización de contenidos basados en el modelo de usuario como herramientas que permiten a los usuarios navegar por la red de un modo cómodo y eficaz. Se veía también que éstas implican necesariamente el uso de determinada información para su correcto funcionamiento. Analizando la Política de privacidad de Google se ha hecho notar cómo en todo momento se le informa al usuario sobre el uso que se va a hacer de su información así como los medios de los que dispone para mitigar tal uso.

De la investigación se ha desprendido el hecho que Google respeta la privacidad de los usuarios-compradores en términos de control, cuando les permite gestionar determinada información personal; de acceso, al introducir claves, contraseñas y preguntas de seguridad en sus servicios; y de acceso restringido, mediante las herramientas que permiten la edición de contenidos y de nuevo con las claves y contraseñas. En este punto se ha señalado el uso de cookies en el ciberespacio. Se ha visto cómo algunas de estas cookies no vulneran la privacidad de los usuarios en la medida en que son necesarias para el correcto funcionamiento de navegación. Sin embargo, se veía cómo otras, como podían ser las cookies de terceros, pueden conllevar una pérdida de privacidad. Las políticas encaminadas a proteger la privacidad de los usuarios se han mostrado insuficientes para hacerlo de un modo efectivo.

Cuando se ha analizado Google a la hora de hablar de privacidad en público y de privacidad como conocimiento de información personal no documentada se ha visto que el problema fundamental para hablar en estos términos en el ciberespacio, y por lo tanto en Google, radicaba en una concepción de la privacidad que se ha dicho analógica. Como espacio eminentemente público, hablar de privacidad en el ciberespacio conlleva problemas que tienen difícil solución, al menos desde la perspectiva de la red superficial. El análisis de la privacidad entendida como conocimiento de información personal no documentada, que en el contexto de esta investigación se ha entendido por ésta el tráfico web, no ha dado resultados concluyentes que puedan afirmar que el uso de ese tipo de información personal sea una invasión de la privacidad injustificada.

En la medida en que las diferentes propuestas teóricas no parecían dar respuesta aplicada a las cuestiones relativas a la privacidad en el ciberespacio, así como tampoco permitían hablar de una pérdida o un uso indebido de la información de los usuarios por parte de Google, se ha propuesto redefinir el concepto de privacidad, que se ha convenido en llamar privacidad digital, para intentar solventar algunos de los problemas que se han visto irresolubles desde las perspectivas teóricas aportadas.

Se ha propuesto una definición de privacidad digital de mínimos, que permita mantener la privacidad de los usuarios centrándose en lo que realmente es relevante de proteger. Además, la definición de privacidad digital dada permite que los usuarios- productores continúen construyendo el ciberespacio así como seguir ofreciendo a los usuarios-compradores los productos que demandan y desean encontrar en la red. Por otra parte, es un concepto de privacidad que en cierta manera aúna todas las propuestas analizadas en esta investigación al tiempo que exime a Google de algunas de las responsabilidades que se le critica no atender.

Se ha visto que es un tipo de privacidad informacional, debido a que se desarrolla en un espacio que también se ha dicho basado en el informacionalismo. Como privacidad característica del tercer entorno, perteneciente a la sociedad red, es una privacidad que pierde, en cierta manera, la distinción entre público y privado. La privacidad digital se dirige hacia aquella información que está en el ciberespacio sólo de un modo secundario y se aleja de toda información que es esencialmente digital y ciberespacial. Sólo protege aquella información digital privada.

Se proponía como información digital privada: las contraseñas, la documentación digitalizada, la mensajería y la información digital confidencial. Todos estos tipos de datos tienen en común que no pertenecen al ciberespacio. La información que contienen no es digital sino digitalizada. Las contraseñas y claves de acceso no forman parte del ciberespacio en la medida en que son las herramientas que dan paso a él. Su participación en este medio es secundaria. La documentación digitalizada que se almacena en la red tampoco forma parte de este espacio. El hecho de que sea almacenada en la nube no significa que participe del ciberespacio, éste sólo es el medio en el cual está alojada esa información. Con la mensajería se veía que ocurre lo mismo. La tecnología sólo es el medio utilizado para enviar un mensaje personal que, por definición, en virtud de estar dirigido a una persona o a un grupo de personas determinado, no tienen carácter público. Es una conversación entre un emisor y un receptor y el ciberespacio debe actuar sólo de canal comunicativo.

Por último, dentro de este tipo de información digital privada se veía aquella considerada información confidencial. Dentro de ésta estaría los informes médicos, los datos bancarios y todo tipo de información sensible. Aquí se mantiene la normatividad del segundo entorno que especifica que se ha de respetar este tipo de información ajena. Por otra parte, sucede lo mismo que con la documentación digital privada o la mensajería. El hecho de que sea información digitalizada no la convierte en información digital. Los bancos o los hospitales y centros de salud digitalizan la información para que ésta ocupe menos espacio, sea más manejable y pueda ser mejor tratada. Pero eso no significa que pueda ser compartida en el ciberespacio. No es una información perteneciente a este entorno, sino al segundo, aunque utilice la tecnología del tercer entorno para gestionarse.

Como se ha visto, esta privacidad deja fuera de su alcance toda aquella información propiamente digital. Dentro de este tipo de información estaría la que se genera por el uso de la red, esto es, la relativa al tráfico web y a la huella digital de los usuarios. Los datos generados por el uso de la red pueden quedar fuera de la protección de la privacidad. En primer lugar, se decía, porque no son relevantes para la privacidad de los individuos. En segundo lugar porque, al dejarlos fuera, permiten continuar con el funcionamiento actual del ciberespacio, que se ha visto beneficioso para todas los agentes involucrados. En tercer lugar, porque al hacerlo, la privacidad digital respondía a muchas de las cuestiones planteadas por la ciberética, y este era el objetivo principal de la investigación aquí presentada.

BIBLIOGRAFÍA
Y
RECURSOS

Obras citadas

- Allen, A. (1988). *Uneasy access: privacy for women in a free society.* New Jersey: Rowman & Littlefield.

- Arhippainen, L. & Tähti, M. (2003) Empirical Evaluation of User Experience in two Adaptive Mobile Application Prototypes. Comunicación presentada en *Proceedings of the 2nd International Conference on Mobile and Ubiquitous Multimedia (MUM), 10-12 de diciembre*. Norrköping, Suecia.

- Aristóteles (2000) *Ética nicomáquea. Ética eudemia.* Traducido por Julio Pallí Bonet. Madrid: Editorial Gredos.

- Barnes, J. (febrero, 1954) Class and Committees in a Norwegian Island Parish. *Human Relations 7* (1), 39-58. doi: 10.1177/001872675400700102

- Been, S. (1984). Privacy, freedom, and respect for persons. En Ferdinand David Schoeman (ed.), *Philosophical Dimensions of Privacy. An Athology.* ed. Nueva York: Cambridge University Press. doi: 10.1017/CBO9780511625138.009

- Bjerén, K. (coord.) (2003) *La experiencia del usuario*. Madrid: Anaya Multimedia.

- Blanke, T. (junio, 2005). Ethical subjetification and search engines: ethics reconsidered. *International Review of Information Ethics, 3,* 33-38. Recuperado de http://www.i-r-i-e.net/inhalt/003/003_full.pdf

- Brin, S. y Page, L. (abril, 1998). The Anatomy of a Large-Scale Hypertextual Web Search Engine. *Computer Networks and ISDN Systems, 30* (1-7), 107-117. doi: 10.1016/S0169-7552(98)00110-X

- Cameron, J., Clarke, R, Davies, S., Jackson, A., Prentice, M. y Regan, B. (1992) Ethics, Vulnerability and Information Technology. *Ethics of Computing: Codes, Spaces for Discussion and Law 2,* (2), 344-350. Recuperado de http://dl.acm.org/citation.cfm?id=660352

- Castells, M. (2006). *La sociedad red: una visión global*. Traducido por Francisco Muñoz de Bustillo. Madrid: Alianza Editorial.

- Castells, M. (2001). *La galaxia Internet* (1a ed.). Barcelona: Plaza & Janés Editores.

- De Bustos, E. (2006). Metáforas de la individualidad moral y fundamentos de la infoética. *Isegoría, 34*, 47-61. Recuperado de https://dialnet.unirioja.es/ejemplar/151696

- Echeverría, J. (1999). *Los señores del aire. Telépolis y el Tercer Entorno* (1a ed.). Barcelona: Ediciones Destino.

- Feltrero, R. (2006). Ética de la computación: principios de funcionalidad y diseño. *Isegoría, 34,* 79-109. Recuperado de https://dialnet.unirioja.es/ejemplar/151696

- Floridi, L. (noviembre, 2002). On the Intrinsic Value of Information Objetcs and the Infosphere. *Ethics and Information Technology, 4* (4), 287-304. doi: 10.1023/A:1021342422699

- Franceschet, M. (junio, 2011). PageRank. Standing on the shoulders of giants. *Communications of the ACM, 54* (6), 92-101. doi: 10.1145/1953122.1953146

- Fried, C. (enero, 1968). Privacy. *The Yale Law Journal, 77* (3), 475-493. doi: 10.2307/794941

- Fried, C. (1984) Privacy (a moral analysis). En Ferdinand David Schoeman (ed.), *Philosophical Dimensions of Privacy. An Athology.* ed. Nueva York: Cambridge University Press. doi: 10.1017/CBO9780511625138.008

- Gavison, R. (enero, 1980). Privacy and the Limits of Law. *The Yale Law Journal, 89* (3), 421-471. Recuperado de http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957

- Górniak-Kocikowska, K. (2007). From Computer Ethics to the Ethics of Global ICT Society. *Library Hi Tech, 25* (1), 47-57. doi: 10.1108/07378830710735858.

- Górniak-Kocikowska, K. (junio, 1996). The Computer Revolution and the Problem of Global Ethics. *Science and Engineering Ethics, 2* (2), 177-190. doi: 10.1007/BF02583552

- Helsten, L., Leydesdorff, L. y Wouters, P. (diciembre, 2006). Multiple presents: how search engines rewrite the past. *New Media & Society, 8* (6), 901-924. doi: 10.1177/1461444806069648

- Hinman, L. (junio, 2005). Esse est indicato in Google: Ethical and Political Issues in Search Engines. *International Review of Information Ethics, 3,* 19-25. Recuperado de http://www.i-r-i-e.net/inhalt/003/003_full.pdf

- Johnson, D. (1996). *Ética informática* (1a ed.). Madrid: Universidad Complutense de Madrid.

- Lanier, J. (2014). ¿Quién controla el futuro? (1a ed.). Traducido por Marcos Pérez Sánchez. Barcelona: Debate.

- Levy, S. (2001). *In the Plex. How Google Thinks, Works, and Shapes our Lives*. Nueva York: Simon & Schuster.

- Lisón, C. (2007). *Introducción a la antropología social y cultural. Teoría, método y práctica.* Madrid: Akal.

- Moor, J.H. (1999). Just consequentialism and computing. *Ethics and Information Technology 1,* 65-69. Recuperado de http://www.idt.mdh.se/kurser/computing/DVA417/Lectures/Moor.pdf

- Moor, J.H. (octubre, 1985). What is Computer Ethics. *Metaphilosophy,* 16 (4), 266-275. doi: 10.1111/j.1467-9973.1985.tb00173.x

- Moor, J.H. (septiembre, 1997). Towards a Theory of Privacy in the Information Age. *Computers and Society, 27* (3), 27-32. doi: 10.1145/270858.270866

- Moor, J.H. (verano-otoño 1990). The Ethics of Privacy Protection. *Library Trends, 39* (1 y 2), 69-82. Recuperado de https://www.ideals.illinois.edu/bitstream/handle/2142/7714/librarytrendsv39i1-2h_opt.pdf?sequence=1

- Nissenbaum, H. (noviembre, 1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy, 17* (5), 559-596. doi: 10.1023/A:1006184504201

- Parent, W. (otoño, 1983). Privacy, Morality, and the Law. *Philosophy & Public Affairs, 12* (4), 269-288. Recuperado de http://philpapers.org/rec/PARPMA

- Parent, W. (diciembre, 1983). A New Definition of Privacy for the Law. *Law and Philosophy, 2* (3), 305-338. Recuperado de https://www.jstor.org/stable/3504563?seq=1#page_scan_tab_contents

- Pariser, E. (2011) *The Filter Bubble*. *What the Internet is Hiding from you*. Londres: Penguin Books.

- Platón (2003). *Diálogos. Obra completa en 9 volúmenes. Volumen III: Fedón. Banquete. Fedro.* Madrid: Editorial Gredos.

- Prenski, M. (octubre, 2001). Digital Natives, Digital Inmigrants. *On the Orizon, 9* (5). Recuperado de http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

- Rachels, J. (verano, 1975). Why Privacy is Important. *Philosophy & Public Affairs, 4* (4), 323-333. Recuperado de http://benjaminferguson.org/wp-content/uploads/2013/01/Rachels-1975-Philosophy-and-Public-Affairs.pdf

- Requena, F. (2003) El concepto de red social. *REIS 48,* 137-152. Recuperado de http://www.reis.cis.es/REIS/PDF/REIS_048_08.pdf

- Sterling, B. (1999). *La caza de Hackers. Ley y desorden en la Frontera Electrónica.* Traducido por El equipo de traductores de Kritópolis. Recuperado de http://kamita.com/misc/sf/the_hacker_crackdown.pdf

- Singer, P. (1984). *Ética práctica* (1a ed.). Gran Bretaña: Cambrigde University Press.

- Spinello, R. y Tavani, H. (2004). *Readings in Cyberethics* (2a ed.). USA: Jones and Bartlett Publishers.

- Suárez Sánchez Ocaña, A. (2012). *Desnudando a Google. La inquietante realidad que no quieren que conozcas*. Barcelona: Deusto.

- Tavani, H. (marzo, 2002). The uniqueness debate in computer ethics: What exactly is at issue, and why does it matter?. *Ethics and Information Technology, 4* (1), 37-54. doi: 10.1023/A:1015283808882

- Tavani, H. (junio, 2005). Search Engines, Personal Information and the Problem of Privacy in Public. *International Review of Information Ethics, 3,* 39-35. Recuperado de http://www.i-r-i-e.net/inhalt/003/003_full.pdf

- Toffler, A. (1970) *El shock del futuro*. Traducido por J. Ferrer Aleu. Barcelona: Plaza & Janés Editores.

- Turkle, S. (1995). *La vida en la pantalla. La construcción de la identidad en la era de Internet* (1a ed.). Traducción de Víctor Viano. Barcelona: Ediciones Paidós.

- Turkle, S. (2012). *Alone Together: Why We Expect More from Techonology and Less from Each Other.* Nueva York: Basic Books.

- Van Couvering, E. (julio, 2004). New Media? The Political Economy of Internet Search Engines. Comunicación presentada en *The Communication Technology Policy section 2004, Conference of the International Association of Media & Communications Researchers (IAMCR), 25-30 de julio.* Porto Alegre, Brasil.

- Vaughan, L. (junio, 2003). New measurements for search engine evaluation proposed and tested. *Information Processing and Management, 40* (4), 677-691. doi: 10.1016/S0306-4573 (03)00043-8

- Vaughan, L. (junio, 2003). Search Engine Coverage Bias: Evidence and Possible Causes. *Information Processing and Management, 40* (4), 693-707. doi: 10.1016/S0306-4573(03) 00043-8. doi: 10.1016/S0306-4573(03)00063-3

- Westin, A. (mayo, 1968). Privacy and Freedom. *The ANNALS of the American Academy of Political and Social Science, 377* (1), 196-197. doi: 10.1177/000271626837700157

- Wiener, N. (1985). *Cybernetics or Control and Communication in the Animal and the Machine* (4a ed.). USA: MIT Press.

- Wouters, P., Helsten, L. y Leydesdorff, L. (octubre, 2004). Internet time and the reliability of search engines. *First Monday, 9* (4). Recuperado de http://pear.accc.uic.edu/ojs/index.php/fm/article/view/1177/1097

Obras consultadas

- Alonso, A. y Del Arco, J. (2006). Para una estética del software libre. *Isegoría, 34*, 167-177. Recuperado de https://dialnet.unirioja.es/ejemplar/151696

- Bardone, E. (2006). La moralidad de las tecnologías cotidianas. *Isegoría, 34*, 179-192. Recuperado de https://dialnet.unirioja.es/ejemplar/151696

- Bush, V. (2001). Cómo podríamos pensar. *Revista de Occidente, 239,* 19-52. Recuperado de http://biblioweb.sindominio.net/pensamiento/vbush-es.html

- Echeverría, J. (2000). Democracia y sociedad de la información. *Isegoría, 22,* 37-57. Recuperado de https://dialnet.unirioja.es/ejemplar/14892

- Echeverría, J. (2003). El principio de responsabilidad. Ensayo de una axiología para la tencociencia. *Isegoría, 29,* 125-138. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=1011506

- Echeverría, J. (2009). Ética y sociedades tecnológicas. *Isegoría, 41,* 217-229. Recuperado de https://dialnet.unirioja.es/ejemplar/252140

- Echeverría, J. (mayo-junio, 2009). Cultura digital y memoria red. *Arbor, 185* (737), 559-567. doi: 10.3989/arbor.2009.i737.313

- Echeverría, J. y González, M. (julio-agosto, 2009). La teoría del actor-red y la tesis de la tecnociencia. *Arbor, 185* (738), 705-720. doi: 10.3989/arbor.2009.738n1047

- Floridi, L. (enero, 2002). What is Philosophy of Information?. *Metaphilosophy, 33* (1-2), 123-145. Recuperado de http://www.jstor.org/stable/24439320?seq=1#page_scan_tab_contents

- Floridi, L. (diciembre, 2002). On the instrinsic value of information objects and the infosphere. *Ethics and Information Technology, 4* (4), 287-304. doi: 10.1023/A:1021342422699

- Floridi, L. (2006). Ética de la información: su naturaleza y alcance. *Isegoría, 34*, 19-46. Recuperado de https://dialnet.unirioja.es/ejemplar/151696

- Floridi, L. (2007). Por una filosofía de la información. *Revista anthropos: Huellas del conocimiento, 214,* 44-50. Recuperado de https://dialnet.unirioja.es/ejemplar/154996

- Gotterbarn, D. (junio, 2001). Informatics and professional responsability. *Science and Engineering Ethics, 7* (2), 221-230. doi: 10.1007/s11948-001-0043-5

- Hindman, M. (2009). *The Myth of Digital Democracy*. New Jersey: Princeton University Press.

- Himanen, P. (2002). La ética del hacker y el espíritu de la era de la información *[versión Adobe Digital Editions]*. Recuperado de http://eprints.rclis.org/12851/1/pekka.pdf

- Magnani, L. (2006). La moralidad distribuida y la tecnología. Cómo las cosas nos hacen morales. *Isegoría, 34*, 63-78. Recuperado de https://dialnet.unirioja.es/ejemplar/151696

- Pan, B., Hembrooke, H., Joachims, T., Lorigo, L., Gay, G y Granka, L. (abril, 2007). In Google We Trust: Users' Decisions on Rank Position, and Relevance. *Journal of Computer-Mediated Communication, 12* (3), 801-823. doi: 10.1111/j.1083-6101.2007.00351.x

- Rogers, R. (2010). Internet Research: The Question Of Method- A Keynote Address from the YouTube and the 2008 Election Cycle in the United States Conference. *Journal of Information Technology & Politics, 7,* 241-260. doi: 10.1080/19331681003753438

- Van Couvering, E. (abril, 2007). Is Relevance Relevant? Market, Science, and War: Discourses of Search Engine Quality. *Journal of Computer-Mediated Communication, 12* (3), 866-887. doi: 10.1111/j.1083-6101.2007.00354.x

Páginas web consultadas

Apple
https://www.apple.com/es/privacy/ Última consulta en agosto de 2016.

Avaaz
https://www.avaaz.org/es/community.php Última consulta en mayo de 2016.

Center for Computing and Social Responsibility
http://www.dmu.ac.uk/research/research-faculties-and-institutes/technology/centre-for-computing-and-social-responsibility/ccsr-home.aspx Última consulta en junio de 2016.

Centro de datos
http://www.centrodedatos-datacenter.es/ Última consulta en agosto de 2016.

Change.org
https://www.change.org/impact Última consulta en mayo de 2016.

Computer Professionals for Social Responsibility
http://cpsr.org/ Última consulta en agosto de 2016.

Diccionario de la Real Academia de la Lengua Española
http://dle.rae.es/?w=diccionario Última consulta en septiembre de 2016.

Electronic Frontier Foundation
https://www.eff.org/es/about Última consulta en agosto de 2016.

El País
http://tecnologia.elpais.com/tecnologia/2006/10/09/actualidad/1160382485_850215.html Última consulta en agosto de 2016.

Google Press
http://googlepress.blogspot.com.es/2004/04/google-acquires-applied-semantics.html Última consulta en junio de 2016.

Google. Privacidad y condiciones
https://www.google.es/intl/es/policies/ Última consulta en septiembre de 2016.

Greenpeace
http://www.greenpeace.org/espana/es/Trabajamos-en/Parar-la-contaminacion/Electronicos/El-problema/ Última consulta en julio de 2016.

International Business Times
http://www.ibtimes.com/android-vs-ios-whats-most-popular-mobile-operating-system-your-country-1464892 Última consulta en julio de 2016.

International Center for Information Ethics
http://icie.zkm.de/ Última consulta en agosto de 2016.

Instituto Nacional de Estadística
http://www.ine.es/ Última consulta en mayo de 2016.

Microsoft
https://privacy.microsoft.com/es-es/privacystatement/ Última consulta en agosto de 2016.

Naciones Unidas
http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf Última consulta en agosto de 2016.

Reporteros sin Fronteras
http://www.rsf-es.org/ Última consulta en agosto de 2016.

Reuters
http://www.reuters.com/article/us-doubleclick-google-idUSN2039512220071220 Última consulta en agosto de 2016.

Search Engine Watch
https://searchenginewatch.com/ Última consulta en agosto de 2016.

Sea-Me-We3
http://www.smw3.com/smw3/SignIn.aspx Última consulta en enero de 2016.

Stanford Encyclopedia of Philosophy. Computer and Information Ethics
http://plato.stanford.edu/ Última consulta en septiembre de 2016.

Techcrunch
https://techcrunch.com/2011/07/20/google-now-the-top-free-app-in-the-apple-app-store/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29 Última consulta en marzo de 2016.

The Wall Street Journal
http://www.wsj.com/articles/SB10001424052748704901104575423294099527212 Última consulta en agosto de 2016.