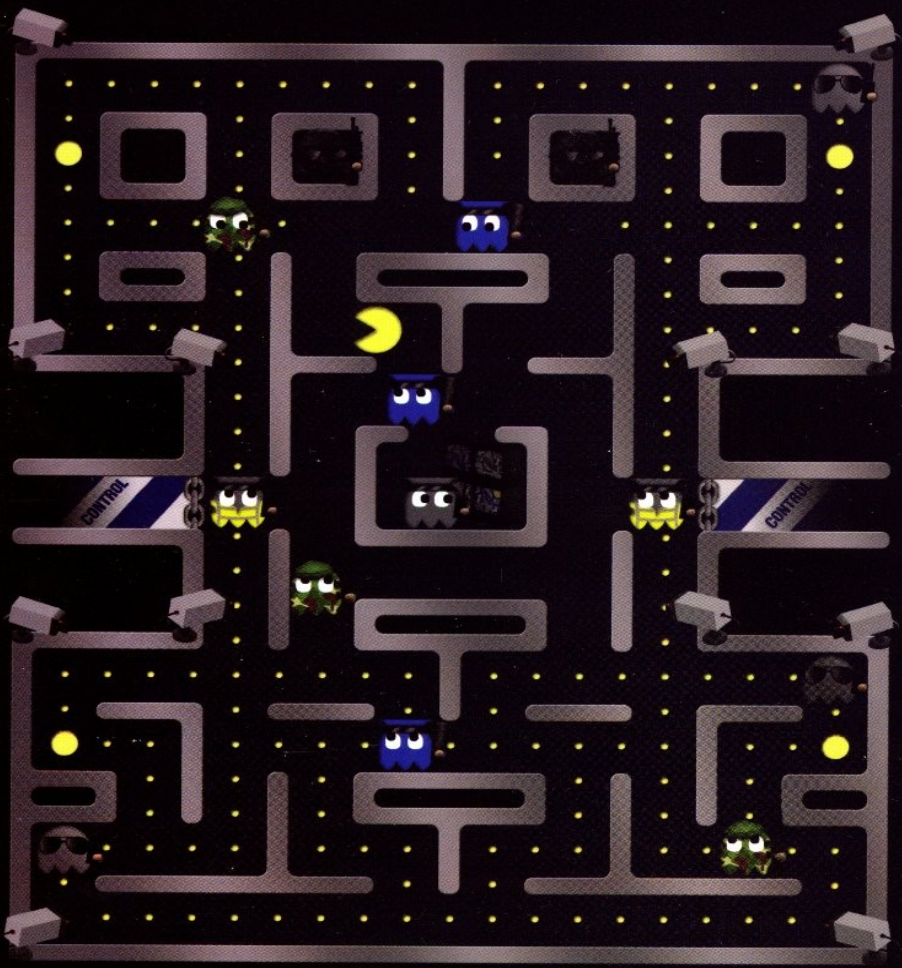
Jose F. Alcántara

LA SOCIEDAD DE CONTROL

Privacidad, propiedad intelectual y el futuro de la libertad

Ediciones ElCobre



La sociedad de control

Privacidad, propiedad intelectual y el futuro de la libertad

Jose F. Alcántara

Colección Planta 29

Primera edición: septiembre del 2008

ElCobre Ediciones

C/ Folgueroles 15, pral. 2ª – 08022 Barcelona

Depósito legal: M-49852-2008

ISBN: 978-84-96501-43-0

Impreso en España

Soy tan sólo uno, pero aún soy uno;
no puedo hacerlo todo, pero aún puedo hacer algo;
y tan sólo porque no puedo hacerlo todo
no rechazaré hacer eso que puedo hacer.

Edward E. Hale

Crearemos una civilización de la Mente
en el Ciberespacio. Que sea más humana y hermosa
que el mundo que vuestros gobiernos han creado antes.

John Perry Barlow

Índice

Sobre el autor

Jose F. Alcántara (Málaga, 1980, info@versvs.net) es consultor especializado en Inteligencia en Internet, comunicación estratégica en la Red y planificación de nuevos negocios y proyectos que puedan aprovechar un uso apropiado de las redes como una ventaja competitiva.

Realizó un doctorado en Química Láser, pero se especializó en las implicaciones sociotecnológicas de Internet en la vida de las personas y la consultoría para el aprovechamiento de la tecnología para la planificación a largo plazo, el desarrollo personal y empresarial, ámbito en el que explota el conocimiento acumulado tras quince años de actividad en Internet y al que se dedica por completo desde hace ya varios años. Actualmente es consultor en el Grupo Cooperativo de Las Indias y vive en Madrid.

Aunque *La sociedad de control* (El Cobre, 2008) es su primer libro, también es autor de *La neutralidad de la Red* (El Arte de las Cosas, 2010).

Información general sobre este libro

Qué puedes hacer con este libro

Este libro ha sido escrito por Jose F. Alcántara, quien hace entrega de él al *Dominio Público*.

Puedes, sin permiso previo del autor, copiarlo en cualquier formato o medio, reproducir parcial o totalmente sus contenidos, vender las copias, utilizar los contenidos para realizar una obra derivada y, en general, hacer todo aquello que podrías hacer con una obra de un autor que ha pasado al dominio público.

Qué no puedes hacer con este libro

El paso de una obra al dominio público supone el fin de los derechos económicos del autor sobre ella, pero no de los *derechos morales*, que son inextinguibles. No puedes atribuirte su autoría total o parcial. Si citas el libro o utilizas partes de él para realizar una nueva obra, debes citar expresamente tanto al autor como el título y la edición. No

puedes utilizar este libro o partes de él para insultar, injuriar o cometer delitos contra el honor de las personas y en general no puedes utilizarlo de manera que vulnere los derechos morales del autor.

Créditos

La portada de este libro ha sido realizada por Fernando Díaz.

La corrección de este libro es obra de Yolanda Gamio.

Agradecimientos

A David, a Natalia y a todos en Las Indias porque sin ellos no habría sido posible, porque creyeron desde el principio en esto y porque sirven de inspiración al movimiento.

A Eva Sánchez por vigilar tantos frentes activamente, porque sus aportes han sido siempre abundantes en mi particular travesía bloguera y porque ha aportado tantos matices a este libro, que no podría pagarlo de otra forma que no sea con mi más sincero agradecimiento; el dinero no sirve.

A Solenne, por todas las conversaciones y todas las alegrías compartidas que nunca nadie contará en ningún libro.

Introducción

Desde que era adolescente soñaba con escribir un libro, quizá uno repleto de poemas; seguramente una novela, siquiera una breve. Siempre pensé que acabaría escribiéndola; eso habría estado bien. Sin embargo, tengo entre mis manos un ensayo alejado de todas esas historias que yo quería contar y lleno de todas las que nadie querría tener que contar. Sólo ahora, con este ensayo entre mis manos, me doy cuenta de lo esquiva que, una vez más, ha demostrado ser la realidad.

Cuando uno se decide a leer un ensayo sobre la privacidad, lo primero que necesita es que le justifiquen por qué debe existir un ensayo sobre la privacidad, que alguien le explique con palabras que todos podamos entender qué

tiene la privacidad que la hace merecedora de un ensayo que la defienda. Es, no le parezca lo contrario, una necesidad idéntica a la que siente el ensayista cuando decide desarrollar su ensayo en torno a un tema que define más que ningún otro el nuevo reto que el entorno digital en el que desarrollamos nuestra vida impone a las democracias funcionales contemporáneas: el derecho fundamental a la privacidad.

El punto de partida es el cambio que hemos experimentado en nuestra sociedad. El mundo ha cambiado tanto en los últimos cuarenta años, que pretender que modelos sociales y económicos antiguos sigan rigiendo la sociedad en la que vivimos constituye una actitud tan irresponsable como reprobable. Y, ¿qué modelo debe servir para organizar una sociedad digital? Pues no lo sabemos, y eso es lo que necesitamos saber. Hasta este momento no se ha decidido nada y todo es posible, precisamente porque no se han desarrollado aún modelos que permitan adaptar nuestra sociedad a nuestro nuevo entorno.

Sin embargo, aquellos que ahora tienen una posición dominante, viejos monopolistas de la información y miembros del poder económico, intentan por todos los

medios apuntalar su influencia en este nuevo entorno y ya han comenzado a presionar a los gobiernos para que legislen a su favor, de modo que nos llevan cierta ventaja.

Pero el que exista un grupo que pretende obtener una posición dominante favorece la organización de un segundo grupo que actuará en oposición al primero: la reacción social, que pretenderá defender sus propios intereses. Estas dos posturas son antagónicas. Y esto define la situación en la que nos encontramos actualmente. Dos grupos sociales, cada uno defendiendo sus propios intereses. Dos maneras de ver la sociedad digital. Una visión restrictiva, una visión abierta. En ambos bandos hay aliados que pueden parecer casuales, pero esta casualidad desaparece en cuanto usamos el criterio adecuado para definir a ambos bandos: los que quieren que la libertad recaiga por igual sobre todos y los que quieren que un grupo, más o menos numeroso, ostente el poder e imponga sus criterios al resto. Los anarquistas y los oligarcas, como los define el profesor Vaidhyanathan.[1]

Por todo esto creo que la privacidad necesitaba una monografía; bueno, por todo esto y porque dedicarle un poco de tiempo a la cara menos amable de la tecnología nos

ayudará a desdibujar toda esa aureola de bondad mística que los medios le han atribuido. Porque la tecnología no es buena ni mala, es una herramienta y será lo que nosotros hagamos de ella. Escribo esta monografía porque de otros usos de la tecnología ya se habla bastante en casi todas partes.

A menudo el debate público sobre nuestra privacidad parte de una premisa completamente falsa, que evidentemente guía el debate por un camino inadecuado e inútil, pues nadie está preguntando por el asunto sobre el que se está respondiendo. La premisa falsa es que el deseo de privacidad nace del deseo de esconder trapos sucios. Esos trapos sucios pueden ser de cualquier índole, porque un trapo sucio es cualquier cosa que esté mal vista por una parte de la sociedad: homosexualidad, corrupción, filiación política o tendencias religiosas.

Esta semántica de combate no es para nada casual, ya que está diseñada para que aquellos que decidimos alzar nuestra voz y exigir un derecho tan básico como es la privacidad más elemental seamos contemplados indistintamente y de forma súbita como terroristas, pederastas, traficantes, *hackers* o delincuentes habituales.

Nadie debería extrañarse de que los medios traten de pintarnos a todos de negro; al fin y al cabo, ellos tienen sus televisiones y en ellas los debates se hacen en los términos que ellos convienen y con las voces que ellos eligen. Lo que sucede es que, ante una situación en la cual una persona o un grupo de personas desea mantener un control sobre los aspectos de su vida que son mantenidos en privado, la única solución que se propone consiste en tratar de equiparar a ese grupo de personas con delincuentes; qué tipo de delincuentes es algo que averiguaremos más adelante, pero lo que es seguro es que se les tildará de delincuentes.

¿No es más fácil pensar que simplemente desean mantener su vida privada sólo al alcance de quien ellos elijan? ¿No es acaso lo que todos hacemos cada día cuando decidimos a quién contamos nuestros asuntos y a quién no? En este caso, como en muchos otros, la explicación más sencilla es la correcta, y defender la propia privacidad no es cosa de terroristas y pederastas, sino más bien de ciudadanos preocupados por los derechos civiles. Tanto las empresas como los Estados rigen su actividad bajo el principio de gestión del riesgo, en lo que se conoce como el mercado de limones y melocotones (una teoría económica

sobre los sistemas de información asimétrica en mercados que le valió a George Akerlof la concesión de un premio Nobel de economía en 2001).[2] Toda información sobre las personas es añadida a un perfil, que será analizado para juzgar si se considera a las mismas un riesgo elevado o reducido. Aquellos que sean incluidos en las categorías de mayor riesgo serán progresivamente apartados de la actividad social y económica (no serán contratados, no podrán obtener seguros médicos ni seguros de vida), pudiendo ser incluso completamente excluidos de la sociedad.

Podría considerarse entonces que, pese a la relevancia que los cambios sociales que hemos vivido han tenido y tendrán en el modo en que se organiza nuestra sociedad, las reclamaciones de privacidad no han sido multitudinarias, y las que han tenido lugar han sido a menudo fraccionadas. Esto se debe a que las nuevas formas de vigilancia y control son juzgadas a menudo desde las supuestas ventajas que ofrecen y no como agentes de penalización. Podemos juzgar que usar un correo webmail como el de Google (que en los términos del servicio exige permiso para leer el contenido de los mismos) supone

entregar a una compañía privada la llave que abre toda tu vida, pero muchos dirán que Gmail es un servicio web magnífico, cómodo y fiable. Esto divide a la población en una infinidad de subgrupos de consumo a la vez que impide su respuesta única y contundente como grupo social. Esta misma situación se dará en torno a otros sistemas como la videovigilancia ciudadana o la constante identificación personal a la que nos vemos sometidos. En todos los casos la respuesta social contundente es minada desde un principio gracias a un habilidoso diseño de la vigilancia, que incita a juzgar estos sistemas en función de sus supuestas bondades y no en función de sus sobradamente probadas capacidades punitivas.

Sé que supone un problema hablar de privacidad. Es cierto: hablar sobre libertad, sobre asuntos éticos, sobre responsabilidades y sobre conveniencia es pedirle a la sociedad que piense en cosas y problemas que preferiría ignorar. Esto puede causar malestar y algunas personas pueden rechazar la idea ya de partida tan sólo por eso. Deducir de lo anterior que la sociedad estaría mejor si dejáramos de hablar de este tipo de cosas es un error que no debemos cometer. Cualquiera de nosotros podría ser el próximo excluido en aras de la eficiencia social.

Como todo avance que tiene lugar a alta velocidad, la llegada de las redes, Internet y todo lo que englobamos bajo el generoso apelativo de nuevas tecnologías nos ha situado, como sociedad desarrollada y permeable a todos estos avances, en una encrucijada, la encrucijada que conlleva toda tecnología: un número enorme de ventajas cuya enumeración sería pesada y aburrida, pero acompañadas de un afilado reverso que nos podría cortar si no actuamos con mesura. La tecnología nunca es neutral y la llegada de la tecnología en sí misma no es un catalizador de mejoras. Si queremos mejoras, debemos luchar porque la tecnología se use y se aplique de forma adecuada.

La privacidad es un derecho moderno. En el siglo XVIII, cuando tuvieron lugar las revoluciones republicanas que sustentaron y dieron origen a las democracias modernas, no había necesidad de privacidad como hoy la entendemos y es por eso que ni se exigió ni se obtuvo en aquel momento. Tendemos a pensar que nos están robando la privacidad. Puede que en la práctica sea así, pero en la teoría es un enfoque equivocado y la realidad es justamente la contraria: la realidad es que la privacidad, tal y como la defendemos ahora, no ha existido jamás porque jamás hizo falta. Y no hizo falta porque nunca un Estado, un tirano o una corporación tuvo las herramientas necesarias para mantener bajo control y bajo vigilancia a toda la población en todo momento, incluso en los momentos en que las personas permanecían solas y aisladas del resto de la población. Esto ni siquiera era posible conseguirlo con un grupo importante de la población.

Pese a los intentos por controlar la privacidad del «partido» y sus colaboradores en los regímenes comunistas totalitarios, la vigilancia a gran escala no ha sido viable hasta la revolución tecnológica digital. Aun así, todos esos esfuerzos eran de «baja tecnología», y ya presagiaban lo que

ahora nos concierne: más allá de que nuestra Constitución reconozca ciertos derechos, es necesario que las leyes que se formulan tomen estos derechos como algo serio que no debe ser pisoteado. La privacidad es un derecho que hay que conquistar. La ley orgánica de protección de datos es un pequeño paso en la dirección adecuada, pero tiene tantas excepciones para invalidarla y tantos aspectos mejorables, que no es en absoluto suficiente.

Sin embargo, con las tecnologías actuales, que cada vez son más baratas, mantener a la población bajo vigilancia es posible y costeable (y será cada vez más barato). Acumular masivamente datos sobre las personas es algo que se puede hacer y que no se puede limitar con tecnología, sino con leyes. La privacidad es un derecho, y utilizar sistemas de cifrado de correo, como el cifrado de clave pública, o de navegación anónima, como Tor, es una buena solución a corto plazo. Son buenas herramientas temporales, necesarias y válidas hasta que consigamos lo que realmente necesitamos: medidas legales que regulen el uso de la tecnología y su influencia en nuestras vidas. ¿Dónde puede haber un chip RFID? Y aún más importante, ¿dónde no puede llegar ese mismo chip? ¿Dónde pueden y dónde no

pueden instalarse sistemas de videovigilancia? ¿Qué condiciones de control será posible imponer por vía contractual? ¿Cómo se regulará el conocimiento de nuestra información genética y bajo qué condiciones no se nos podrá exigir que cedamos esa información? ¿Qué hay del secreto de nuestras comunicaciones?

En el presente libro haremos una revisión de algunos de los frentes en los que se está desarrollando más activamente la defensa y la violación de nuestra privacidad. Intentaremos analizar cómo se ejerce el poder y quién lo ejerce; para esto resulta muy interesante observar las teorías que contemplan la vigilancia y el uso estratégico de la información como una herramienta para obtener el poder. Comenzaremos situando la privacidad en su contexto, aportando información básica (qué es la privacidad, qué es la sociedad de control). Un segundo bloque comprenderá el análisis de las tecnologías de control en algunos de sus ámbitos más habituales (desde el espionaje público hasta los estudios publicitarios). El tramo final del libro abordará el estado legal de nuestra privacidad y transmitirá unas pautas para defenderla (tanto en el plano más interno -nuestra propia privacidad- como en el ámbito

más social: ayudar a que otros tomen conciencia de su privacidad).

La privacidad es un derecho civil contemporáneo porque los problemas y las tecnologías que la ponen en peligro son contemporáneos. Y los derechos nunca se regalan, es algo que hemos aprendido de la historia; los derechos, hasta los más elementales -quizá éstos aún más-, hay que ganarlos. Eso es algo que en este país sabemos bien. ¿Está preparado para exigir reformas que garanticen nuestra privacidad?

1. Privacidad

La Real Academia Española de la Lengua define *privacidad* como el «ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión».[3] La privacidad es todo lo que tenemos derecho a reservar para nosotros mismos o, visto desde un punto de vista mucho más pragmático, todo lo que tenemos derecho a que los demás no sepan de nosotros. El término «todo» utilizado en la oración anterior puede parecer en exceso general, incluso atrevido. No es para nada atrevido. La privacidad está en todas partes. Allí donde hay actividad humana existe el derecho a controlar la forma en que esa actividad será transmitida y dada a conocer al resto del mundo, en caso de que queramos que ésta sea transmitida y comunicada. Existe también el derecho a que esa actividad no sea conocida por nadie más que las personas que la efectúan.

Hay quien afirma que el término «privacidad» no es sino una mala traducción del vocablo inglés *privacy*, «intimidad». Sin embargo, y pese a su gran similitud, podemos matizar diferencias. Si consideramos que la intimidad es la «zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia»,[4] podemos atisbar claramente diferencias con lo que

anteriormente definimos como privacidad. La privacidad no es algo que se tenga derecho a reservar, sino el derecho mismo a reservar algo para nosotros mismos.

La diferencia entre estos dos conceptos podemos subrayarla aún más utilizando un ejemplo: el de las ideologías políticas. El que una persona tenga una determinada posición política es algo que tiene derecho a mantener en privado, más aún en situaciones en que eso pueda poner en peligro su empleo o su seguridad, pero sin duda no es algo íntimo, pues el fin último de una idea política es precisamente un fin público: que la sociedad se organice de una manera determinada. Así pues, privacidad e intimidad no son equivalentes. No todos los ámbitos de la privacidad pertenecen realmente a la intimidad, aunque sí que todas las actividades de nuestra intimidad estarían bajo el paraguas de la privacidad, y tenemos derecho a protegerlas todas.

El que la privacidad adquiera relevancia está vinculado al desarrollo de la sociedad digital en la que los países más ricos e industrializados están completamente inmersos. Cuando en los años sesenta aparecieron las primeras computadoras, la población supo de inmediato que

dichos inventos tendrían la capacidad de almacenar enormes cantidades de datos, pero no se preocupó por su privacidad, sólo porque en aquel momento introducir una pequeña cantidad de datos requería mantener a una gran cantidad de personas trabajando con tarjetas perforadas. Así que la vigilancia global y personalizada no era viable y no se le dio importancia.[5] Actualmente sabemos que todo lo que hace falta para almacenar la información relativa a todas las actividades de una enorme cantidad de personas es un ordenador personal: éstos cuestan alrededor de quinientos euros y se puede tener una docena de ellos en una pequeña habitación. Y nadie ve nada. No parece un precio elevado y unas condiciones que dificulten que eso suceda. Y con el advenimiento de Internet y la creciente implantación de infraestructuras para telecomunicaciones digitales cada vez son más las actividades que desarrollamos en red, y que son susceptibles de ser registradas.

La lucha por la privacidad es la lucha por asegurar que en un futuro podamos hacer las cosas que queramos sin miedo a represalias. Aunque haya quien afirma, como Scott McNealy,[6] que «la privacidad ha muerto»,[7] a nosotros nos parece que es un bien necesario que podría ser cada vez más

valioso. Es, por tanto, un bien a preservar por el valor que tendrá para nuestra sociedad en un futuro donde todo será trazable.

La lucha por la privacidad es también la lucha por decidir quién puede saber qué sobre nosotros, quién puede almacenarlo y bajo qué condiciones, y cuándo y bajo qué condiciones puede alguien acceder a ello. La lucha por la privacidad es la lucha por elucidar la legitimidad de las enormes bases de datos con información personal que día a día se crean y van creciendo en nuestra sociedad para saberlo todo sobre nosotros. Aunque suene grandilocuente, la lucha por la privacidad es la lucha por volver a equilibrar las democracias. Las democracias se basan en el respeto mutuo entre gobierno y pueblo, y la sociedad digital y las posibilidades que ofrece hacen que sea necesario un nuevo análisis con objeto de garantizar que la democracia siga siendo respetada. La lucha por la extensión y el respeto de la privacidad es la lucha por elevar y mantener una serie de barreras que permitan adaptar la democracia a la era digital sin alienarla, defendiendo por encima de todo su esencia: la libertad del pueblo.

1.1. ¿Cuándo existe un problema de privacidad?

Para ubicar de forma precisa el problema que vamos a analizar es relevante que sepamos de qué hablamos cuando nos referimos a un *problema de privacidad*. No toda información supone un peligro para nuestra privacidad. Aclarar la situación y acotar aquello que nos va a suponer un problema será de gran utilidad porque nos permitirá concentrarnos en solucionar esos problemas técnica y legalmente, dejando de lado la disputa por asuntos que no nos suponen un verdadero problema y que restarían tiempo y dedicación a aquello que realmente lo merece.

La situación se puede explicar de forma muy sencilla utilizando el ejemplo de la Viagra, de Pfizer. Tomemos como ejemplo a una persona que compra una caja de las pastillas azules más famosas de los últimos veinte años. Desde el momento en que una persona, sujeto 1, decide comprar estas píldoras, pueden darse varias situaciones. En primer lugar, que alguien decida comprar estas pastillas no constituye en sí mismo un problema de privacidad; resulta obvio, pero hay que decirlo. En segundo lugar, puede que alguien, sujeto 2, sepa que se han vendido unas pastillas

pero no tenga posibilidad alguna de conocer la identidad del comprador; esto tampoco constituiría un problema de privacidad y puede ayudar a ese sujeto 2, por ejemplo la farmacia o su gerente, a llevar un control eficiente de su inventario, pero no constituye un problema de privacidad. En un tercer caso, puede que alguien, de nuevo un sujeto 2, tenga en su mano la posibilidad de vincular la identidad del comprador con el producto comprado. Este tercer caso sí supone un problema de privacidad.

Aunque parezca irrelevante o lejano, esto sucede cada día. Sucede cuando usted va al supermercado y decide pagar con su tarjeta de crédito o su tarjeta de fidelidad o de comprador frecuente («la tarjeta de los puntos»). Sucede cada vez que usted va a comprar CD vírgenes o un libro y le exigen sus datos para crear una ficha de cliente. Puede que para algunas personas estas acciones no supongan una preocupación; muchas personas piensan que el problema no va con ellos porque no les importa quién pueda saber que compraron *Cien años de soledad*. No parece un asunto de vida o muerte, no parece nada vinculado a conspiraciones ni a extremismos políticos, religiosos ni raciales. Ahora hágase, por favor, la pregunta a la inversa: ¿De verdad necesito

identificarme cuando voy a comprar *Cien años de soledad*? Claro, visto así no podemos decir que exista una justificación. Y ahora vaya un poco más lejos y piense que, en algunos países, comprar un Corán, *El libro rojo de Mao* o el *Mein Kampf* estaría mal visto y podría granjearle la enemistad de alguno de sus vecinos o compañeros de trabajo, de su jefe o, en algunos entornos más duros, de su propio gobierno, incluso aunque usted sólo los haya comprado para saber cómo pensaban algunas de las mentes que más problemas crearon en el pasado siglo XX; aunque sólo quiera tener sus textos sagrados en casa, del mismo modo que otras muchas personas tienen una Biblia.

Evitar que cualquiera pueda saber todo sobre nosotros se presenta, entonces, como una necesidad. Llamémoslo prevención de riesgos civiles, un camino para poner a salvo nuestra sociedad si llegaran tiempos difíciles. Ahora ya sabemos qué son los problemas de privacidad y entrevemos un poco por qué nos interesa evitarlos. En las páginas que quedan por venir hablaremos en profundidad sobre estos asuntos.

1.2. Tipos de problemas

Ahora ya no hará falta que siga imaginando: todos sabemos que, a raíz de los atentados del 11-S contra el World Trade Center, se han aprobado una gran cantidad de medidas que permiten la vigilancia de la ciudadanía en nombre de la seguridad. La verdad es que muchas de estas medidas ya estaban en marcha antes del 11-S y el atentado no fue lo que originó su aplicación, pero sí posibilitó que oscuras medidas de vigilancia desconocidas por la mayoría de la sociedad salieran a la luz pública y fueran aceptadas en tiempos de crisis, algo imposible bajo otras circunstancias.

Un ejemplo de una de estas aplicaciones son las listas negras para el embarque en aviones que el gobierno de Estados Unidos confecciona utilizando un software de trazado de perfiles, las llamadas *no-fly list*. La lista se trazó de forma automática haciendo minado de datos de telecomunicaciones e Internet por parte de la Agencia Nacional de Seguridad (NSA, National Security Agency) de Estados Unidos. Esa lista es tan extensa que incluye unos cincuenta mil nombres, e incluso aparecen en ella senadores y ex-miembros del gobierno.[8] ¿Cree que las posibilidades de ver su nombre en dicha lista habrían aumentado

sensiblemente de aparecer en su perfil de compras (o en su *lista de deseos*) de Amazon alguno de los tres libros antes mencionados? Con un mal uso del minado de datos, y es el que se suele hacer, es muy probable que así sea. La identificación de personas que realizan compras aparentemente inofensivas supone un problema de privacidad. Estos problemas de privacidad y limitación de derechos están actualmente tan extendidos, que esbozar un análisis de los ámbitos más relevantes en que la presentación de algún tipo de credencial nos posibilita (o nos impide) realizar hasta la más insignificante de nuestras actividades diarias ocuparía todo un libro.

No todos los problemas de privacidad se relacionan con asuntos de seguridad nacional, espías y atentados terroristas. Una cara menos temida, aunque igualmente indeseable, de la vulneración de nuestra privacidad es la invasión publicitaria de todos los espacios públicos y privados. Las nuevas técnicas de publicidad se apoyan drásticamente en el conocimiento íntimo del cliente, generando una gran cantidad de información que podría ser susceptible de abuso. Y es que desde la calle por la que paseamos hasta nuestra estación de metro, la página web

donde miramos nuestras noticias o nuestros propios electrodomésticos, todo es susceptible de incluir mecanismos que sirvan para enviar al publicista información sobre qué cosas nos gustan y cómo las usamos. Con la invasión publicitaria, pronto cualquier dispositivo será capaz de mostrar anuncios o «consejos» que, para mayor inquietud, utilizarán información sobre nosotros a fin de adaptarse a nuestros hábitos de consumo y aficiones. De esta forma, los publicistas lograrán ofrecernos anuncios optimizados, cuyo porcentaje de éxito será mayor, y nosotros gastaremos más dinero.

1.3. ¿Qué genera estos problemas?

Dado que las causas que generan conflictos con nuestra privacidad son tan heterogéneas, no será fácil agrupar todo aquello que atañe a este asunto de forma que su análisis sea realmente sencillo.

Entre los causantes de estos problemas, elementos y sistemas que permiten o facilitan vincular nuestras actividades y nuestra identidad, destacaremos las tecnologías de control, como la identificación por radiofrecuencia (RFID, Radio-frequency Identification), la

videovigilancia o la gestión de restricciones digitales (DRM, Digital Restrictions Management), las medidas legales (traza privada sin control judicial, retención de datos de telecomunicaciones privadas, ley de propiedad intelectual) y, en un apartado diferente pero de la mayor importancia, nuestros hábitos diarios y el uso que hacemos de nuestros datos personales en la red y fuera de ella. Nuestros hábitos, a menudo descuidados en lo que se refiere a proteger nuestra información personal, suponen una ventana abierta por la que se ve minada nuestra privacidad.

1.3.1. La tecnología

Resulta sencillo comprender por qué la tecnología es una de las fuentes de este tipo de problemas. El progresivo abaratamiento de la misma facilita su extensión, y su extensión facilita la tendencia natural de todo poder establecido a usar ese poder para perpetuarse indefinidamente.

El desarrollo de enormes entramados urbanos formados por videocámaras y los cada vez más frecuentes lectores de RFID son una buena muestra de esta tendencia. La vigilancia de las telecomunicaciones, la retención de

datos, el análisis de tráfico en la red, la traza sin control judicial y el minado de datos acumulados son un claro ejemplo de cómo la tecnología, alimentándose básicamente de nuestras actividades en Internet, se convierte en una herramienta que ataca nuestra privacidad.

Un problema añadido es que estos modos de operación, lejos de estar bajo control público, están la mayor parte de las ocasiones bajo control privado. No es que el hecho de que puedan estar bajo control público sea tranquilizador -no lo es-, pero al menos al vivir en una democracia podemos pedir cuentas a nuestros gobernantes. Resulta mucho más difícil imponer a una empresa privada qué puede y qué no puede hacer, pues no tiene miedo a perder unas elecciones y, si tiene monopolio suficiente, tampoco tendrá miedo a perder clientes obligados a serlo por falta de opciones.

Sólo la ley puede ayudarnos en esa ardua tarea, pero ya sea por desconocimiento o por negligencia (yo apuesto a una alta influencia de este segundo motivo) existen vacíos legales en la mayoría de ámbitos relacionados con la privacidad y desconocimiento acerca del problema. Las posibilidades abiertas al abuso de la tecnología nos llevan

mucha ventaja.

1.3.2. La legislación

Para enmarcar y cerrar debidamente la definición de «problema asociado a la privacidad» sólo nos falta mencionar el hecho de que los problemas de privacidad no son un problema técnico, o al menos no lo son ni mayoritaria ni únicamente. Los problemas de privacidad son problemas legales. Ya que disponemos hasta cierto punto de herramientas técnicas que permiten mitigar, sólo en parte, el efecto de todo lo mencionado anteriormente sobre nuestra privacidad, el verdadero problema no siempre es poder hacerlo o no, sino impedir que se nos acose constantemente. El fondo de la cuestión es que la ley debería regular cierto tipo de actuaciones y limitar la cantidad de información que se puede recoger sobre las personas, así como su uso.

Iniciar una carrera técnica entre el desarrollo de tecnologías de control y medidas para evitarlas no solucionará el problema; no lo ha hecho hasta el día de hoy y no lo hará en el futuro. Lo que realmente necesitamos son leyes. Pero para que se promulguen esas leyes hace falta que

la sociedad conozca este problema, tome conciencia real del mismo y traslade esta inquietud a los políticos, que finalmente se encargarían de desarrollar leyes que cumplan el deseo del pueblo. Está claro que todo este proceso ideal se complica cuando vemos que políticos y grandes medios de comunicación no están interesados en que este tema se someta a un debate público o ignoran premeditadamente la voluntad popular, como sucede en los asuntos relativos a la restricción de copia. Pero esta cerrazón exhibida desde el poder no debe hacernos perder el verdadero sentido de todo este movimiento. El movimiento por la defensa de la privacidad persigue únicamente el desarrollo de leyes que protejan este derecho.

1.3.3. Las personas

Por último, aunque no menos importante, están los riesgos para nuestra privacidad que son consecuencia de una conducta no apropiada. La tecnología es una herramienta y sirve para aquello que la apliquemos. Es justo reconocer que la tecnología que hace posible que nos bombardeen con publicidad también ha conseguido desarrollar los mecanismos que nos permiten evitar dichos bombardeos.

Los servicios publicitarios invasivos y la extensión de sistemas de identificación personal como videocámaras, RFID o sistemas de reconocimiento biométrico siempre irán un paso por delante, como consecuencia de una simple lógica dialéctica, pues no podemos ignorar un tipo de publicidad ni de vigilancia que no conocemos y para el que no nos hemos preparado. Aun así, tenemos herramientas suficientes para bloquear, ignorar y reducir el impacto de la mayoría de estos sistemas que socavan nuestra privacidad.

Por simple y molesto que parezca, uno de los mayores problemas de privacidad que tenemos es culpa exclusivamente nuestra y reside principalmente en lo poco que valoramos nuestros datos personales, algo que nos lleva a no evaluar adecuadamente las consecuencias de muchas de nuestras acciones cotidianas, que de otra manera juzgaríamos imprudentes o irresponsables. Suscripciones a cualquier revista gratuita, una tarjeta de fidelidad que promete servirnos de mucho ahorro o la inscripción gratuita a cualquier concurso, todo ello sirve para recolectar nuestros datos, que por lo general valoramos muy poco. La ingeniería social sigue funcionando mejor que cualquier otra técnica para recolectar datos sobre nosotros (datos de

carácter personal, de consumo de productos, de uso de productos).

Confiamos en la simplicidad. Los cada vez más habituales servicios web, que nos prometen ubicuidad a cambio de conservar toda la información relativa a nuestras actividades, aprovechan el valor de la simplicidad que nos ofrecen (no debemos preocuparnos por mantener sincronizada la información en todas nuestras computadoras) para recoger toda la información relativa a nuestro día a día. En los casos en los que un mismo proveedor ofrece múltiples servicios web, el valor de la información aumenta al permitir armar el puzzle completo de nuestra vida, pero nosotros la regalamos igual de barata.

Ante esta situación, de nada sirve que la tecnología ofrezca mecanismos para proteger la información si al primer desconocido que nos pregunta nuestros datos para un concurso de dudosa fiabilidad le proporcionamos nuestro nombre, el DNI, el número de teléfono y el correo electrónico; por si ganamos, claro. Cuando se trata de la privacidad, nuestra conducta es una fuente de problemas que no deberíamos despreciar y representa la mayor vía de agua en nuestra navegación.

1.4. ¿Cómo evitar muchos de estos problemas?

Dado que gran parte de nuestros problemas provienen de nuestra propia conducta, lo más importante y lo primero que necesitamos hacer para evitar muchos de nuestros problemas de privacidad es aprender a valorar nuestra información personal. La tecnología puede ayudar: ya hemos dicho que del uso que le demos dependerá lo que obtengamos de ella, pero sólo servirá de algo cuando contemplemos esta tecnología como algo que nos beneficia por la protección que nos ofrece. Y para ello lo principal es ser conscientes de que nuestra información personal es muy valiosa.

Para esta tarea valoraremos las medidas de prevención (evitar costumbres que no nos benefician y entregan mucha información), sin olvidar las medidas de presión (cada euro que gastamos apoya algo; podremos apoyar a aquellos que nos respetan como personas y como clientes) y las medidas técnicas (cifrado asimétrico, software libre).

Sobre todas ellas volveremos a lo largo del ensayo. Lo principal es saber que, aunque no podemos evitarlo todo,

sí hay muchas cosas que están bajo nuestro control. Necesitamos reclamar en primer lugar el control de todo aquello que, como hilos, vamos dejando suelto por ahí. Una vez lo hayamos logrado, estaremos preparados para ir más allá y comenzar a recuperar una parte de nuestra intimidad y nuestra privacidad arrebatadas.

2. La sociedad digital

Definir en unas pocas líneas todo lo que es y supone la sociedad digital es más una temeridad que una odisea, pero vamos a acometer el desafío e intentar trazar unas líneas que sirvan de patrón para definir las principales diferencias entre este nuevo mundo completamente conectado y un mundo anterior que carecía de todas las infraestructuras digitales y tecnológicas actuales. Usaremos la comparación porque estamos preparados para entender con toda facilidad un mundo en el que nos hemos criado y en el que se nos ha enseñado a vivir.

Me referiré al momento actual y a las posibilidades sociales que las nuevas tecnologías nos ofrecen como

sociedad digital. Lo haré porque ésta es la principal diferencia entre nuestra sociedad y la situación de la que venimos. Resulta habitual leer referencias a la *sociedad de la información*. No faltan argumentos a favor y en contra de esta expresión, mucho más empleada; sin embargo, resulta errónea si consideramos que en todas las civilizaciones y sociedades que ha habido a lo largo de la historia la información siempre ha sido valiosa. Por eso he preferido un nombre distinto; algunos autores prefieren llamarla *sociedad red*. No me aventuraré a divagar sobre la revolución digital ni nada parecido. La sociedad digital ofrece nuevas oportunidades, pero aún hay que darle forma y fijar los principios básicos de respeto a las libertades que harán posible el cambio. El mundo actual, pese a las posibilidades que las redes ofrecen, y que poco a poco van surgiendo y madurando, es esencialmente muy parecido al mundo tal y como ha sido siempre.

Merece la pena hacer hincapié en que, gracias a los avances en tecnología digital y a la creciente capacidad de producir y almacenar más información con un coste realmente bajo, se inicia una carrera por producir y gestionar la información, aumentando su valor intrínseco.

Aquellos que puedan emerger de esta cerrera con más fuerza dentro del mar de creación de información tendrán en sus manos la posibilidad de influir en la sociedad al contar la realidad a través de su propio prisma. Esto es posible en la actualidad asumiendo unos costes realmente bajos, lo que hace que los canales tradicionales de distribución de información, esencialmente limitados por la barrera de entrada económica a los mismos, pierdan peso específico. Pero a pesar del cambio en la distribución, la información ya estaba ahí cuando los clérigos controlaban quién estudiaba con ellos y quién no, o cuando hicieron falta las revoluciones republicanas del siglo XVIII para que se implantaran sistemas educativos públicos que los reyes absolutistas de toda Europa se negaban a aceptar. Eso ya era valorar la información y la capacidad de acceso y distribución de la misma. Justo lo que la sociedad digital está cambiando; justo lo que muchos quieren dejar inmutable, retrasando el cambio y generando una gran multitud de problemas que poco a poco van captando la atención de la población.

2.1. El cambio a lo digital

A comienzos del siglo XX ni siquiera sabíamos que

los átomos (cuyo nombre evoca su supuesto carácter indivisible) estaban divididos en aquello que se definió con las analogías macroscópicas de núcleo y corteza, ni que era esa corteza la que contenía unas partículas extremadamente pequeñas con carga eléctrica negativa que, una vez descubiertas, fueron llamadas electrones. Ése es el mundo en el que vivíamos. Cuando lo llamamos «analógico» hay que tener presente que a las cosas no se las llamó analógicas hasta que aparecieron otras similares que funcionaban de forma distinta y que denominamos digitales. Hace algo más de medio siglo el mundo en el que vivíamos era lo que hoy llamaríamos un mundo completamente analógico. El mundo tal y como nos lo contaron de pequeños.

La gran diversidad de sociedades y civilizaciones que han poblado el planeta nos sirve en bandeja un rico abanico de costumbres y sistemas económicos y de comercio; sin embargo, son sorprendentemente reducidos los principios en los que todas estas sociedades apoyan sus sistemas económicos. Las distintas sociedades humanas tienen, por encima de toda diferencia, un punto en común: la manufactura de bienes físicos es el objeto de toda industria y se emplea para aumentar el valor de los

productos. La compra y la venta de objetos físicos es el fin de todo comercio. En un sentido amplio, esta manufactura podría incluir también sectores como el agrícola o el ganadero, si consideramos en estas actividades la manufactura no como el proceso de darle forma a algo, sino como el proceso de cultivo o crianza de animales y plantas.

Dos cosas diferenciarán a la sociedad digital: por una parte, el bien activo de mayor valor no es un bien material, sino algo tan intangible como la palabra que usamos para comunicarnos, la información; por otra parte, los canales que sirven para transmitir esa información han cambiado radicalmente su topología; ahora tenemos canales distribuidos.

La información puede ir encapsulada en algún soporte material, aunque no es una condición necesaria y esto sucede cada vez menos, sobre todo en el caso de según qué tipo de información y de contenidos. Estos soportes pueden ser periódicos o discos compactos, por citar algunos, pero no es el soporte el que les confiere su valor. Cuando compramos un diario no pagamos un euro por unas hojas de papel y tinta, pagamos un euro para conocer la actualidad de nuestro entorno, ya sea nuestra ciudad, nuestro país o las

noticias internacionales.

Pero también hemos dicho que en la sociedad digital los canales de acceso a la información son distribuidos. Lo que esto quiere decir es que, más allá de unos cuantos nodos bajo control estatal o de grandes empresas que intentan controlar la agenda pública y las noticias que llegan a nuestros oídos, en la sociedad digital cada persona tiene la posibilidad de ser un nodo de información, de transmitir su visión sobre asuntos que de otra forma no llegarían a la opinión pública y permitir el acceso a esa información a quien quiera acceder. La sociedad digital modifica el modo en que la arquitectura de transmisión de la información se organiza.[9]

No es nada nuevo que la información tiene un elevado valor y la capacidad de acceso a la misma ha sido la causa de luchas en múltiples ocasiones. Las revoluciones sociales de los siglos XVIII-XIX contaron como uno de sus grandes éxitos la implantación de sistemas de acceso a la información. Los sistemas educativos públicos y otros mecanismos de acceso gratuito a la cultura, como las redes de bibliotecas, tienen su origen precisamente en esta época. Las revoluciones sociales, que también sirvieron para

provocar el nacimiento de las democracias modernas, centraron su lucha en la obtención de un poder para el pueblo y centraron su éxito en la obtención de un sistema de acceso a la información, la educación y la cultura pagado por el conjunto de ciudadanos a través del Estado, a fin de asegurar que el pueblo, alejado de la ignorancia, pudiera mantener los derechos recién adquiridos.

El paso hacia la modernidad, marcado por las revoluciones estadounidense y francesa, y que se dio también en otros países, vino definido por el acceso masivo de la población a la cultura gracias a los sistemas educativos implantados en aquellos países donde iban teniendo lugar. Obtener ese acceso no fue sencillo y casi cualquier intento de conseguirlo acabó en revueltas violentas y guerras internas, guerras por el acceso a la información y a la cultura.

2.2. La información como un bien valioso caro de reproducir

Información es casi cualquier cosa en la que usted piense, no sólo televisión, radio y noticias. Un libro de texto es información, igual que una novela o un poemario.

También son información la última película de Steven Spielberg y el último documental de Julio Medem, así como el último álbum musical que usted haya copiado y la anotación más reciente de su blog preferido.

En la sociedad previa a la tecnología digital e Internet el precio a pagar por acceder a la información derivaba de dos factores diferentes: al valor que la información poseía en sí misma había que añadir inevitablemente los costes de producción, replicación y distribución, pues era inevitable que esta información estuviera sujeta a algún tipo de soporte material. Si tomamos el ejemplo de un libro, éste debe estar fabricado en papel y fabricar ese papel cuesta dinero. Además, aunque desde la invención de la imprenta los costes de producción se habían reducido y ya no había que emplear a dedicados y cuidadosos escribanos para reproducir los libros, todavía hacía falta comprar la imprenta, el papel y la tinta, ensamblar el libro y permitir que toda la cadena, desde el autor hasta el librero, obtuviera un beneficio que les permitiera continuar con su actividad.

Para el asunto que nos incumbe, cada copia del libro tendrá el mismo coste de producción que dependerá de las

materias primas empleadas. De esta forma, cada copia tendrá un precio de puesta a disposición del cliente que permitirá que las obras más vendidas den un mayor rendimiento económico. Según esta teoría, un autor superventas tendrá más beneficio que uno que venda unas pocas copias. Sin embargo, en la época en que apareció la sociedad digital, el sistema de comercialización de obras culturales se había concentrado tanto, que había degenerado. Esta alta concentración, sobre todo en la música, posibilita la imposición de contratos abusivos a los artistas. De esta forma, en un entorno en el que el mercado cultural genera más ingresos que ningún otro, rara vez estos autores reciben una compensación acorde a los beneficios que reportan a los grandes editores, que controlan de forma casi total el mercado de novedades culturales. Nótese que pese a que también existe una gran concentración en el mercado literario, éste sufre menos intensamente dicho control.

Es por esta elevada concentración del mercado, y por los abusos que permitía, por lo que la sociedad digital está molestando tanto a estos editores: les está rompiendo un sueño, el sueño de decidir qué pueden leer y escuchar

millones de personas en todo el mundo, y cuánto van a pagar por ello. Por supuesto, como veremos más adelante, la situación de libertad de tránsito y adquisición de información y cultura podría ser transitoria; es algo que tanto las empresas del sector como los gobiernos están buscando por numerosas vías. La gran mayoría de estas vías invaden nuestra privacidad o limitan nuestros derechos y, por tanto, son inaceptables. De hecho, la forma en que se ha enfocado la lucha por recobrar el control de la información es tan violenta, que el debate está en la calle y parece improbable que la sociedad acepte estas nuevas imposiciones sin antes olvidar todo lo que sabemos de nosotros mismos y de nuestra ética social, con los peligros que ello conllevaría.

2.3. La información digital como un bien valioso barato de reproducir

La información digital, en ausencia de formatos físicos, es barata de producir y distribuir, y a pesar de ello resulta no sólo codiciada, sino que además es el activo de mayor valor en la sociedad digital.

La sociedad digital se caracteriza por un hecho

singular: el coste de producción del primer ejemplar de cualquier tipo de información (recordemos que información puede ser cualquier cosa, como ya hemos mencionado más arriba) es en la práctica el coste total de producción de todos los ejemplares que se quieran producir. El coste de la copia es marginal y en ello reside una diferencia básica e importante con respecto a los sistemas de producción no digitales. El coste de producción y distribución de la segunda copia de cualquier información (incluidas películas, libros y álbumes musicales) será cero siempre que consideremos un formato electrónico para nuestra copia.

Los costes de producción totales de una obra se relacionan con la producción del primer ejemplar; básicamente, con el tiempo empleado para su creación, ya que la tecnología para llevar a cabo numerosas creaciones está tan disponible, que comparativamente no supone un coste adicional, y menos aún una barrera para dicha creación. Si consideramos como ejemplo la creación de un álbum musical, éste atraviesa hasta su producción final por un arduo proceso e composición, ensayo y grabación. Igualmente, la redacción de un artículo periodístico conlleva una documentación previa y la propia escritura del artículo.

Este mismo libro requerirá un buen número de horas de elaboración y documentación antes de alcanzar su estado final y que usted pueda leerlo.

Adicionalmente, cada vez más, en la generación de información los costes de producción se derivan únicamente del tiempo necesario para la producción, debido al abaratamiento progresivo y la mayor disponibilidad de la tecnología. Mientras que un grupo musical antes debía alquilar un estudio y caros equipos de grabación, ahora puede grabar por sí mismo su música con una computadora y su propio equipo de sonido, cada vez más baratos en los países desarrollados; para escribir una novela no hace falta, actualmente, más que una computadora, cuyo precio puede rondar los quinientos euros. Por supuesto, tanto la novela como la música requieren además muchas horas de trabajo, pero todas esas horas de trabajo son necesarias para la producción de la primera copia de la obra, del original. Toda esa elaboración se incluye en los costes de producción, pero afecta solamente a la producción de la primera copia. Las sucesivas copias no tendrán coste alguno si nos decidimos por una versión electrónica.

El hecho de que ahora una información, del tipo que

sea, vaya en un determinado soporte se puede considerar, desde este punto de vista teórico, un lujo, casi un atavismo social, y por tanto normalmente exige el pago de una cantidad de dinero. Pero ello no significa que no haya otras formas de distribuir la información que no estén sujetas a estos soportes y cuyo precio no pueda ser mucho menor. No hay necesidad de comprar una película o un álbum musical en un soporte físico. Usted podría adquirirlo de forma digital, copiarlo en su propio equipo y, si lo considera necesario, hacer una copia local en soporte físico. Este soporte físico tiene un coste, pero al no tener que pagar la elaboración y la distribución remota de esa copia física desde -quizá- la otra parte del mundo, el coste sigue siendo marginal y asumible. Los costes seguirían recayendo en la producción del original. El coste de producir las copias seguiría siendo nulo y, en consecuencia, el dinero ya no se obtendrá de la venta de las mismas. Cuando la barrera para producir información disminuye y la información es abundante, el dinero no sigue la ruta de las infinitas copias producidas a coste cero, sino que sigue la ruta de la atención y recompensa a aquellos capaces de generar algo novedoso, sin recompensarlos necesariamente mediante la venta de sucesivas copias de ese algo.

2.4. El surgimiento de la sociedad digital: la red

Lo comentado anteriormente no es suficiente para provocar el nacimiento de la sociedad digital. La sociedad digital no existiría sin las redes, y la aparición de las redes define el cambio. La revolución tecnológica digital y su repercusión en el modo en que nos comunicamos y el modo en que creamos, transmitimos y almacenamos información no eran, en sí mismas, una revolución. Hacía falta un paso más. Claro que el paso no estaba tan lejos y ya desde los orígenes de la informática existía en los investigadores el deseo de conectar máquinas, el deseo de conseguir que esas máquinas se comunicaran entre sí, el deseo de formar redes.

Desde su origen militar la red evolucionó y se extendió hasta llenarlo todo. De la batalla por controlar y conectar los satélites que vigilan al enemigo la red se ha extendido a empresas y hogares. En los países desarrollados la red está tan presente, que a menudo olvidamos lo que era nuestro día a día sin ella. Alentadas por las posibilidades de anunciarse a un bajo coste, las empresas se han ido dotando de una presencia en Internet y aquellas que no lo han hecho han dejado escapar una ocasión. La libertad de la red, el

acceso a información lejana, la facilidad de comunicación, la instantaneidad del correo electrónico, estos fueron los motivos que atrajeron a la gente. La posibilidad de aumentar en unas decenas de euros la factura mensual de millones de clientes fue el principal impulso que las empresas del sector de las telecomunicaciones vieron para llenar de fibra óptica nuestras ciudades. Entre todos construimos la red: unos construían la infraestructura con el apoyo de los distintos Estados y otros llenábamos la red haciéndola cada *vez* más interesante y atrayendo cada vez a más personas. De las listas de correo a los chats, la mensajería instantánea y los blogs. «La red engancha», decían las noticias. Sí, la red engancha, pero lo hace porque en la red, al otro lado del cable, hay otra persona que está contando su visión de las cosas; quizá una visión distinta que difícilmente llegaría nunca a la televisión.

2.4.1. Del sistema descentralizado al distribuido

Además de las diferencias señaladas anteriormente, existe una gran diferencia entre los sistemas de comunicación anteriores a la revolución digital y el sistema de información y comunicación que hace posible Internet tal y como está hoy diseñada. El paso a una sociedad digital ha

hecho posible también el tránsito desde un sistema de red descentralizada a un sistema de red distribuida. La red, que hasta ahora sólo unía a Estados y grandes grupos empresariales, llega hasta cada hogar y se convierte no en algo propio de una oligarquía, sino en algo disponible para todos. La red se vuelve social, la sociedad se une a la red. El hecho de que las dos grandes guerras del siglo XX fueran *guerras mundiales* se debió a la estructura de los mecanismos de información derivados de la invención del telégrafo y la creciente conexión entre distintas naciones: un conflicto entre dos naciones ya no podía ser ignorado por el resto nunca más, pues acabaría afectando a las demás, y la comunicación inmediata y las nuevas tecnologías de transporte hacían posible el desplazamiento rápido y coordinado de tropas a lo largo de muchos cientos de kilómetros. Asimismo, la lucha de bloques durante la segunda mitad del siglo pasado atiende precisamente a esta condición: las telecomunicaciones hacen posible que distintas naciones estén informadas en tiempo real de lo que sucede en las demás naciones, y la necesidad de alcanzar acuerdos y coordinarse con los respectivos aliados y hacer frente a las posibles alianzas enemigas se hace imperiosa.

En este punto, la red se comporta como un sistema descentralizado en el que los nodos son tanto Estados como grupos empresariales del sector de las telecomunicaciones. La aparición de la informática y el advenimiento de Internet superan este sistema mediante la creación de infinitos nodos que hacen que la información corra a través de canales distribuidos y fuera del control de los nodos tradicionales (Estados, grupos mediáticos)[10] y dotando a estos nuevos canales distribuidos de una enorme agilidad a la hora de difundir información y organizar protestas como las llevadas a cabo en las numerosas cumbres de líderes mundiales en los últimos años o como la que se produjo en España entre los días 11 y 13 de marzo de 2004.

2.4.2. La estructura técnica de la red. Protocolos y controles.

Aunque formalmente existen una gran cantidad de redes, dado que actualmente hay una infraestructura única que da cobijo a una gran red que acoge en su seno un sinfín de pequeñas redes temáticas, hemos preferido hablar de la red en singular, de Internet, aunque esa red sea en sí misma una red de redes.

Si tenemos que hablar de la red y de sus

características estructurales, hemos de comenzar mencionando que la red fue diseñada por científicos y, en tanto que criatura de la ciencia, se rige por sus principios. La red está diseñada para ser funcional, y de este interés por dotarla de funcionalidad derivan dos de sus principales características: la red es abierta y la red es libre. Esto queda perfectamente expresado en la siguiente característica: todas las conexiones de la red se realizan empleando protocolos, que constituyen una sólida base de software libre, los protocolos TCP/IP.

Habituado como estoy desde hace años a utilizar computadoras y la red, en mi vida diaria hace ya mucho que dejé de pensar en qué quieren decir cuando nos dicen que estamos usando un *protocolo*. Escuchamos hablar de ellos a menudo y los utilizamos con aún más frecuencia, pero a menudo no tenemos una idea muy precisa de lo que significan. Sin embargo, hay un símil que sirve para explicar este concepto de forma extremadamente sencilla: un protocolo es un apretón de manos, un acuerdo entre dos partes. Y un protocolo informático es el modo en que dos computadoras llegan a un acuerdo y deciden cómo (orden de envío y cantidad) van a intercambiar información. Lo

opuesto a un protocolo sería un control. Un control es una imposición, de una de las partes sobre la otra, sobre el modo en que se van a hacer las cosas.[11]

Protocolos y controles no son algo exclusivo del mundo digital. Nuestra sociedad funciona gracias a la existencia de un número equilibrado de protocolos y controles, a los que se recurre cuando es necesario. Para que sea más fácil: un juicio es un protocolo, un método desarrollado para encontrar una verdad; una prisión es un control.

La red es caótica y lo es porque su propio diseño lo permite. Los protocolos sobre los que se apoya todo el esqueleto de la red son libres. El software que permite la interconexión y la asignación de una dirección unívoca a cada una de las máquinas de una red es libre. También los protocolos que mueven la web, desarrollados por Tim Berners-Lee, son libres. Todos los sistemas anteriores son libres porque fueron desarrollados por científicos bajo principios científicos y por eso él nunca ha reclamado un control de los protocolos que desarrolló y que hacen posible la web como la conocemos. En palabras del propio Berners-Lee: «La web es una economía de mercado, y en una

economía de mercado cualquiera puede comerciar con cualquiera. Todo lo que necesitan es llegar a unos acuerdos mínimos como la moneda a utilizar y las reglas para un comercio justo».[12] Todo lo que necesitan es seguir un protocolo. Y la red tiene sus protocolos.

La red fue diseñada para facilitar la escalabilidad de la misma, de forma que su crecimiento, la unión de una nueva máquina a la red, no obligase a reiniciarla completamente ni a reconectar de nuevo todos los nodos ya existentes en la red. Ello facilita que cualquiera pueda unirse a la red en cualquier momento, compartir o utilizar sus recursos y luego volver a salir. Esa libertad asusta a quienes tradicionalmente han controlado la forma en que las personas accedían a la información y a muchos otros servicios, desde gobiernos a grupos de prensa y discográficas. Todos ellos ven ahora amenazado su sistema piramidal y centralizado de acceso.

El control oligárquico de unos pocos se ve actualmente minado por el principio que sirvió para diseñar y construir la red: la libertad. Por eso cada paso que los Estados y las corporaciones privadas dan con la pretensión de controlar la red debe ser mirado con recelo. Una red llena

de controles no sólo no serviría a su propósito inicial, sino que permitiría un universo cerrado y censor.

2.4.3. El peligro de rediseñar la red

Los protocolos que rigen la red permiten una gran libertad de acción. La red que nos permite compartir música es la misma que permite a disidentes chinos leer noticias del extranjero que su gobierno censuraría; y es también la misma red que permite a la dictadura china detener a los mencionados disidentes. El diseño de la web permite el intercambio de pornografía infantil; el diseño de la web permite que las fuerzas de seguridad atrapen a los pederastas. La libertad de la red asusta a algunos, que insisten en criminalizarla, sin embargo la red no es ni buena ni mala. La red es lo que hagamos con ella. En otras palabras, los cuchillos no matan a las personas; las personas matan a las personas.

Pero ése no es el mensaje que día a día nos transmiten las noticias. Las noticias no nos hablan de disidentes que evitan la censura de regímenes dictatoriales, ni del acceso a la información y la cultura por parte de una población que, de otra manera, quizá no podría pagar por

ella. Las noticias que nos hablan de Internet nos hablan de pederastia y de *copyright*. Las noticias nos dicen que los terroristas del 11-S y el 11-M usaron Internet unos días antes de los atentados. ¡Pues claro que la usaron! ¡Como millones de personas en todo el mundo! Quizá también usaron un ascensor y comieron fruta, como millones de personas, pero a nadie se le ocurre plantear el cierre de los mercados.

¿Mejoraría la seguridad en la red con un rediseño? No lo sabemos, pero más bien podemos estar seguros de que quienes estén interesados en delinquir, averiguarán cómo hacerlo y dispondrán de los medios económicos para lograrlo. En cambio, los cientos de millones de personas que ni lo hacen ni lo pretenden estarán bajo control, su vida estará vigilada y, si deciden opinar en contra de un gobierno o de una gran corporación, serán observados. No parece que este tipo de controles respete la libertad de expresión tal como nos la garantiza la declaración universal de los derechos humanos.

En Estados Unidos, la coyuntura del 11-S fue utilizada para emprender una cruzada contra la disponibilidad de acceso público a Internet en las

bibliotecas, y más adelante veremos que la amenaza contra las bibliotecas no es una casualidad. Todas esta campaña de declaraciones, todas las acusaciones contra la libertad que nos permite la red son fruto del miedo que las clases dirigentes tienen a la red. Esta persecución no es azarosa; se criminaliza injustamente aquello que se teme. En este caso concreto, los medios y los gobiernos atacan a la red porque la posibilidad de libertad de información y comunicación que abre les produce miedo.

Por absurdo que parezca el comentario, hay que expresarlo por escrito: la libertad no nos convierte en peores personas. La mayoría de la población no cometería un asesinato o abusos contra menores aunque tuviera ocasión de hacerlo; la pequeña minoría de asesinos restante encontraría el modo de llevar a cabo dichos abusos con Internet o sin ella. Es por eso que una herramienta de comunicación libre, en manos de una población que mayoritariamente no tiene pensado cometer asesinatos en serie, es un problema para aquellos que solían controlar los nodos a través de los cuales circulaba la información que moldeaba la agenda pública y sus aspiraciones. Pero eso es precisamente la sociedad digital, un cambio radical en el

modo en que nos comunicamos y accedemos a la información, un cambio radical en la forma en que se determinan la agenda y las preocupaciones públicas, cada vez menos controlada por los poderes político y mediático convencionales.

Frente a la euforia que suelen mostrar algunas personas, es prudente recordar que no todo está decidido sobre la forma en que se estructurará la sociedad digital. Más aún, nada está decidido. No pocas veces hemos oído hablar de que un rediseño de la red haría de ella un lugar más seguro, libre de abusos terroristas y pederastas. Es una retórica muy persistente por parte de los gobiernos y hace hincapié en el argumento más utilizado por nuestros políticos en los últimos años: la seguridad nacional.

Un rediseño de la web es actualmente una empresa faraónica. Los protocolos TCP/IP están en todas partes, desde supercomputadores a pequeños dispositivos con software empotrado. Los utilizan todos los sistemas operativos y actualmente están preparados para ofrecer tantas direcciones (número de máquinas conectadas a la red) como 2^{128}. La casi totalidad de los dispositivos que incorpora tecnología de redes trabaja bajo TCP/IP. Cambiar

el sistema en que funcionan todos y cada uno de los dispositivos del mundo requeriría un gran trabajo de programación y no parece viable a corto plazo.

Sin embargo, no por ello hay que dejar de considerar lo que podría significar. Si la red nos ofrece una experiencia de comunicación única e incomparable con todo lo que podamos tener actualmente, se debe precisamente al modo en que está construida. Un rediseño de la web podría cambiar el sistema actual, basado en protocolos, y reemplazarlo por un sistema distinto basado en controles, un sistema basado en imposiciones en el que unos pocos controlen quién hace qué y cómo, cuándo y dónde pueden hacerlo. Un rediseño de la red es algo tan difícil de hacer como peligroso, y por eso mismo intentarán antes o después abordarlo, porque quienes se resisten al cambio tratarán de recuperar el paraíso de control que acaban de perder. Esta idea será una constante en la sociedad digital en tanto se mantenga libre, y si la libertad tiene un precio es únicamente ése: el de la vigilancia eterna de los factores que podrían arrebatárnosla. Y esta idea será una constante en la sociedad digital porque es una constante en toda sociedad, digital o no, que toda generación debe luchar por defender

sus derechos frente a quienes intentan recortarlos.

3. Sociedad bajo vigilancia

3.1. El origen de las democracias modernas

Pertenezco a una generación que no ha vivido nunca bajo un régimen dictatorial, algo que podríamos tomar como norma histórica y totalmente normal cuando miramos cómo se ordenan los diferentes países de nuestro entorno europeo. Sin embargo, no podemos obviar que las democracias, tal y como las conocemos, son estructuras ciertamente modernas.

Si consideramos la historia más reciente de Europa occidental y otros países ricos, tan sólo a partir de las

revoluciones republicanas del siglo XVIII en Francia y Estados Unidos (esta última les valió la independencia) han existido en Occidente democracias reales. En algunos países, como es el caso de España, ese periodo se reduce mucho más, pues ni siquiera en esta época hemos gozado de una democracia real permanente: de los aproximadamente cincuenta años de democracia que hemos tenido en España, más de treinta los hemos vivido tras la dictadura franquista.

Son precisamente las dos fechas mencionadas, la revolución estadounidense y la revolución francesa, las que marcan según algunos historiadores y expertos en derecho el origen de las democracias modernas,[13] así que tenemos un total de unos doscientos años de democracia, en el mejor de los casos con el añadido de que ésta prácticamente se circunscribe a parte de Europa occidental y Norteamérica. Sin duda parece un periodo de tiempo bastante breve si se compara con toda una historia de siglos repletos de regímenes totalitarios.

La revolución francesa se gestó, como no podía haber sido de otra manera, en París. Uno de los factores que menos en cuenta se tuvieron, incluso por parte de los propios vencedores, en la narración de la revolución

francesa fue que los parisinos gozaron de la posibilidad de burlar el sistema de vigilancia y censura que imponía la monarquía absolutista. La monarquía prohibía agruparse con otros ciudadanos y charlar con ellos; la política no se suponía algo público, sino privado.[14] De esta forma la monarquía se aseguraba de que las ideas de la Ilustración, que comenzaban a extenderse, no pudieran originar rumores ni corrientes de pensamiento que pusieran en peligro el trono de Francia ni el régimen absoluto que se imponía desde el mismo. La prohibición funcionó bien en dos entornos: las ciudades de tamaño mediano, que eran fácilmente controlables, y las zonas rurales, que no requerían vigilancia porque en ellas no había masa ciudadana suficiente para que existieran los peligros derivados del análisis crítico y revisado de las obras ilustradas. Pero el sistema falló en París. La megaurbe y sus grandes jardines hacían posible todo lo que la monarquía borbónica quería prohibir: formar un pequeño grupo, discutir un asunto y perderse entre la muchedumbre. Así sucedía, por ejemplo, en los jardines de Luxemburgo o en el Pont Neuf, así sucedía en numerosos rincones de una ciudad demasiado grande para que el rey pudiera impedir completamente las reuniones de sus ciudadanos.[15]

Por supuesto, la revolución no se habría logrado sólo gracias a esa posibilidad de conversación. Quizá esa posibilidad ni siquiera era imprescindible para que se produjera. Lo significativo es que el régimen autoritario de la época quiso evitarlo porque sabía que suponía un peligro para su estabilidad. Lo significativo es que esta situación facilitó enormemente las labores de organización de los revolucionarios republicanos que introdujeron la democracia en Francia.

3.2. Sociedades bajo vigilancia en el siglo XX

La vigilancia a la que fueron sometidas diferentes sociedades durante el siglo pasado fue la causante de algunos de los episodios más tristes y violentos de dicha centuria. En todas las sociedades y en todos los Estados ha existido siempre un cierto nivel de vigilancia; lo diferente, en los casos de vigilancia masiva, es el patrón seguido para decidir qué y por qué se vigila. Y eso es lo que salió mal en algunos momentos del siglo pasado y eso es lo que está saliendo mal en lo que llevamos de éste.

La vigilancia existe y es una herramienta, y cuando

está bien usada es provechosa: cuando se sospecha de alguien o de algo, se le vigila y de esa manera se ayuda a mantener un cierto orden social que todos agradecemos. En el siglo XX, numerosos Estados y dictaduras de todo signo violaron este principio de seguridad extralimitándose y abusando de esta vigilancia para utilizarla en contra de la oposición política o de personas que no apoyaban explícitamente al régimen dictatorial de turno.

El abuso de esta vigilancia interna nace de la naturaleza dictatorial, percibida como tal o no, de estos regímenes. Una dictadura ve en cada ciudadano un posible enemigo, alguien que en todo momento podría actuar en su contra. Eso hace que los ciudadanos deban ser oprimidos y sus acciones limitadas: es un recurso para la perpetuación del régimen. Los motivos esgrimidos para lograr la colaboración de parte o toda la población son muy diversos y van desde los religiosos (si la dictadura promete preservar los valores religiosos tradicionales, obtendrá el apoyo de grupos de este entorno) hasta los meramente políticos (si las personas piensan que no apoyar a un régimen socialista contribuye a la erosión de los valores sociales y a la derrota del Estado a manos de otros Estados y sistemas).

Pero sobre todo, las dictaduras se apoyan en el miedo de sus ciudadanos hasta convertirlos en súbditos. Dos de los regímenes cuyos ciudadanos han estado más vigilados a lo largo de la historia fueron regímenes idealistas que surgieron en el siglo XX, revoluciones populares que se apoyaron en el propio pueblo para triunfar y que luego utilizaron a ese mismo pueblo para actuar en su contra, causando millones de víctimas.[16] Hablamos del régimen soviético y del chino, dictaduras nacidas de revoluciones idealistas en las que el gobierno optó por volver a robar al pueblo la soberanía recién adquirida para perpetuarse en el poder.

El primero de ellos tardó casi ochenta años en derrumbarse, y las secuelas de los años de los oligarcas de Yeltsin y las actuales políticas de Putin aún recuerdan demasiado a aquella época. El segundo ha migrado del comunismo al libre mercado manteniendo como constante del sistema la opresión del pueblo y la corrupción de sus dirigentes, algo que no tiene visos de cambiar. La sociedad china es un claro ejemplo de sociedad bajo vigilancia en la que las nuevas tecnologías se utilizan para apresar y reprimir a los disidentes.[17] China aplica frecuentemente la

pena capital (más que ningún otro país del planeta) y algunos de los delitos que se castigan con la muerte, como la evasión fiscal, ni siquiera implican violencia.

También se apoyaron en la vigilancia interna de sus ciudadanos las dictaduras del Cono Sur en las décadas de los setenta y ochenta, instauradas gracias a la Operación Cóndor de la CIA, que colaboró con equipos informáticos para facilitar la vigilancia de los disidentes políticos en regímenes dictatoriales como el de Pinochet en Chile.[18]

3.3. La política del miedo

Conocemos como *política del miedo* una nueva manera de entender la política en la cual los discursos políticos no enfatizan las promesas de un futuro mejor, sino que abundan en profetizar el catastrofismo derivado de no obedecer al pie de la letra lo que nos está ordenando el político de turno. Si tradicionalmente la política ha consistido en desarrollar acciones que desembocarían en un futuro mejor y en explicarlas al pueblo para ganar su apoyo, la política del miedo recurre a la seguridad (generalmente la *seguridad nacional*) para obtener el apoyo incondicional de la ciudadanía a una serie de medidas políticas que de otra

forma no serían respaldadas.

En la política del miedo se presentan al pueblo una serie de amenazas difusas y caóticas (como el «terrorismo internacional») como excusa para conseguir que se acepten políticas de recorte de derechos y de vigilancia masiva de la ciudadanía (como el derecho al secreto de las comunicaciones, el derecho a la intimidad o la aceptación de tratos indignos en controles aeroportuarios) a cambio de ayudar a preservar el orden y la fuerza del Estado que *apresa y encarcela a los terroristas*, manteniendo así ese caos profetizado en un segundo plano de la realidad.

La política del miedo es una respuesta a una realidad social: tras décadas de promesas incumplidas, el poder del encanto verbal del político que pretende convencer a la población de que eligiéndolo a él en lugar de a los otros candidatos el mundo se convertirá en un lugar mejor ha desaparecido. Los políticos necesitan algo más para recobrar su influencia y es ahí donde la generación de miedo le gana la partida a las simples promesas de bonanza económica y social.

3.3.1. El origen de la política del miedo

Para buscar el origen de la actual política del miedo hay que viajar hasta mediados del siglo XX. En esa época, en dos sociedades distintas, la occidental y la árabe, algunas personas tendrán ideas y plantearán acciones que desembocarán en la radicalización de las ideologías Dos transformaciones que se oponen como enemigas íntimas, pues se fortalecen en su propio entorno cuanto más se fortalece la opuesta en aquellos lugares donde tiene influencia.

En 1949, el maestro egipcio Sayyid Qutb viajó a Estados Unidos (la nueva tierra prometida tras la victoria en la segunda guerra mundial) con el objetivo de estudiar su sistema educativo. Lo que vio allí le inspiró una serie de ideas que medio siglo después han influido y conformado la visión político-religiosa de grupos islamistas radicales. La sociedad norteamericana de la posguerra mundial, que en Occidente se percibía como una sociedad alegre y optimista tras la victoria aliada, le pareció a Qutb una sociedad en decadencia ética, colmada de un enorme vacío personal y entregada a banalidades (cine, automóviles, etc.) innecesarias. Según Qutb, el materialismo y el

individualismo estaban pudriendo la sociedad estadounidense y, tras su viaje, volvió a Egipto dispuesto a evitar que esta cultura «sucia» se adueñara de su país. Según él, la moral nihilista estadounidense amenazaba el correcto desarrollo de una vida acorde con los preceptos del islam y por eso el medio que ideó para prevenir la entrada de este nuevo nihilismo en Egipto fue devolver al islam un lugar preeminente en la política de su país. Qutb escogió la «politización del islam» para imponer reformas sociales que limitaran la libertad que, según él, amenazaba con devorar al país e impedir el desarrollo de una vida acorde con las normas coránicas. Las ideas de Qutb acabarían teniendo largo alcance, pues con posterioridad a su ejecución en Egipto (acusado de rebeldía) algunos de sus compañeros en los Hermanos Musulmanes decidieron poner en práctica su ideario. Más adelante, ese grupo se convertiría en el embrión del Yihad Islámico. Entre ellos se encontraba Ayman al-Zawahiri, que años más tarde sería mentor y una de las mayores influencias ideológicas de Bin Laden.

Leo Strauss (filósofo, Universidad de Chicago) compartía la visión de Qutb: Estados Unidos se autodestruye, víctima de su individualismo. Strauss pensaba que era

posible detener esta destrucción nihilista y egoísta y para ello propone que «los políticos deben instaurar mitos en los que todos puedan creer; pueden ser mitos falsos si hace falta, pero son, al final, mitos necesarios». Según Strauss, la solución al problema pasaba por la construcción de un nuevo conjunto de ideales que posibilitara la recuperación, por parte de la ciudadanía, de la fe en sus políticos, bastante débil tras las promesas (nunca cumplidas) de «un mundo mejor». Según Strauss, dos mitos serán suficientes para conseguirlo: la religión y la nación. En Estados Unidos esto se tradujo inmediatamente en la idea de que Estados Unidos es el «pueblo elegido» para combatir a las fuerzas del mal en todo el planeta. Se unieron los dos nuevos mitos en uno y se utilizaron de forma indistinta, recurriendo, de camino, a uno de los mitos políticos más antiguos que existen: el de «el pueblo elegido».

De este modo, Strauss produjo el mismo efecto que Qutb había conseguido en los países árabes: la religión se volvía a mezclar con el Estado. Las ideas de Strauss también tendrían largo alcance, ya que, pasado el tiempo, serían las que inspirarían a los denominados neoconservadores, *neocons*, estadounidenses, que durante decenios han estado

ostentando los poderes político y económico de dicho país (Rumsfeld, Cheney, Bush padre) y cuyas ideas se extienden por Europa desde la década de los ochenta gracias al gobierno de Margaret Thatcher en Reino Unido. Como último apunte, mencionar que Strauss ya pensó en la posibilidad de que la elite del país no compartiera el mensaje que transmitía. De hecho, en su opinión, la elite destinada a propagar el mensaje no necesitaba creer en el mensaje: tan sólo debían hacer lo posible para que la ciudadanía sí lo creyera, adoptando en público actitudes que dieran esa impresión.

3.3.2. La política del miedo en la actualidad

En años recientes, y de manera muy acusada desde comienzos del siglo XXI, son los atentados de Nueva York, Washington, Madrid y Londres los que se están utilizando para justificar la mayoría de medidas mediante las cuales se da cobertura a la política del miedo, que han alcanzado cotas de abuso muy elevadas. En este comienzo de siglo esta política se ha extendido por todo Occidente, y concretamente en la Unión Europea es ampliamente utilizada para justificar medidas de control en todos los ámbitos: intercepción de comunicaciones, vigilancia

ciudadana, excesivos controles, reducción de derechos en los aeropuertos e incluso operaciones contra el intercambio de archivos en la red se justifican con los argumentos de la lucha contra el terror y la seguridad nacional. La seguridad es la excusa estrella cuando se requiere una justificación pública de unas actividades que no parecen muy justificables.

Desde el ascenso a lo más alto del poder político de los primeros discípulos de Strauss (entre los que podemos contar a Donald Rumsfeld) a principios de los años setenta se había promovido la idea de que una oscura red de movimientos terroristas alrededor del mundo estaba siendo financiada por Moscú y el bloque comunista de Europa del Este. El objetivo al que apuntaban estas supuestas informaciones era el supuesto interés de este bloque comunista por sumir al mundo en un caos que lo haría desangrarse para posteriormente emerger de este caos y dominarlo. Es interesante porque utiliza un concepto de enemigo difuso y en red que se hará mucho más poderoso cuatro decenios después, en la actualidad.

La caída de la Unión Soviética sin la desaparición del terrorismo hizo necesario reinventar el mito del enemigo.

Tras años de reestructuración propagandística, las agencias de seguridad estadounidenses encontraron una situación asimilable a esta teoría del enemigo difuso, una situación en la cual se nos presenta una amenaza terrorista coordinada, pero ya no bajo las órdenes de Moscú y el bloque comunista, sino bajo control del enemigo islamista. Se trata de una red de la que casi nadie sabe nada y a cuyos líderes nunca se les ve en público, un *enemigo difuso para una guerra larga*.

Este cambio de táctica hizo que la otra parte que está en el origen de esta nueva política, los islamistas politizados seguidores de las ideas de Qutb, que también ganaban adeptos, redefiniera su mito: ahora no es la moral estadounidense la que destruye a los musulmanes, sino los estadounidenses mismos los que destruyen a los musulmanes extendiendo deliberadamente lo que ellos consideran una enfermedad.

En los últimos años, uno y otro bando han radicalizado sus ideas: de los tristes atentados del 11-S al no menos triste uso de armas químicas en Falluya, que causó 35.000 muertos en dos días. Por parte estadounidense, la «guerra contra el terror» se hace fuerte en los medios y comienza a llenar telediarios, portadas de periódicos y

columnas de opinión. De hecho, esta propaganda progresa alarmantemente en ambos bandos, ya que en la polémica y en la guerra tanto los conservadores como los islamistas se aseguran un mayor poder y un mayor control (en tiempos de guerra se pueden exigir al pueblo cosas que de otro modo serían imposibles). Mediante esta confrontación lo que tenemos es una estrategia para perpetuarse en el poder a cualquier precio, cada uno en sus dominios.

El éxito de la política del miedo

Es evidente que estos dos grupos han cambiado el mundo, pero no de la manera que en un principio perseguían. Ambos eran idealistas que rápidamente se dieron cuenta de que estas ideas les devolvían el poder que la política tradicional y sus promesas (nunca consumadas) ya no les volvería a otorgar: el poder de conseguir que el pueblo les obedeciera. Pero, a diferencia de las promesas de antaño, ahora los más influyentes no serán aquellos que prometan el mejor futuro, sino aquellos que, azuzando los miedos más oscuros, puedan conseguir más concesiones de la población.

Tras este cambio en la forma de hacer política, la

doctrina de la guerra preventiva se hace fuerte y se aplica tanto en ámbitos internos como externos. La idea de que para prevenir atentados «desde dentro» hace falta controlar qué hacen los ciudadanos del propio país gana cada vez más adeptos entre los dirigentes políticos de todo el mundo. Suele decirse que esto es consecuencia del 11-S, pero ficha afirmación no es correcta. Estas políticas ya se venían planeando y desarrollando con anterioridad a los atentados de Nueva York y éstos constituyen tan sólo el parapeto, la coyuntura utilizada para consolidar esta política de restricción de derechos y libertades.

La doctrina del shock

La doctrina del shock es el nombre que Naomi Klein da a la ideología económica reformista de Milton Friedman, miembro de la escuela de Chicago y compañero de Leo Strauss en la Universidad de Chicago. Según esta doctrina del shock, la atmósfera creada por una crisis a gran escala provee el pretexto necesario para invalidar los deseos expresos de los votantes y entregarles la economía del país a los tecnócratas.[19] Para la aplicación de la doctrina del shock se requiere por tanto una crisis, casual o inducida, que se pueda sostener durante el periodo de tiempo necesario para

la imposición de estas medidas impopulares.

Se relaciona íntimamente con la política del miedo, pues el shock es por definición un estado transitorio y superable. La política del miedo persigue mantener a la población sumida en un estado de shock para poder llevar a cabo medidas y reformas impopulares.

3.3.3. Las medidas de seguridad

Si algo caracteriza a la política del miedo es la necesidad de oponerse a ese enemigo invisible mediante la implementación de medidas de seguridad y vigilancia que recortan nuestros derechos pero, teóricamente, ayudan a mejorar la seguridad.

Hay una pregunta que es obligatorio formularse en este momento: tras haberse demostrado que la mayoría de estas medidas son completamente ineficaces cuando hablamos de mejorar la seguridad de las personas, ¿de qué están hablando cuando hablan de medidas de seguridad? Aunque la psicología con la que está elaborado el mensaje nos incita a pensar que se habla de nuestra seguridad, está claro que no hablan de nuestra seguridad tal y como la entendemos habitualmente. Las medidas de seguridad que

anuncian a bombo y platillo nuestros gobiernos no nos ayudan a a estar más seguros frente a lo desconocido, sino que permiten un control intensivo y extensivo de las personas por parte de éstos. Las medidas de seguridad no nos defienden a nosotros del enemigo desconocido, sino que defienden a los gobiernos de lo que sus ciudadanos podrían hacer para exigirles responsabilidades.

Este uso confuso y malintencionado del término *seguridad* es el culpable de muchas malinterpretaciones en materia de privacidad, que llevan a la aceptación de medidas restrictivas de los derechos que de otra forma no se aceptarían. Luchar contra este astuto uso de la propaganda política es también parte de lo que tenemos que hacer.

3.3.4. Las netwars

Netwar es el nombre que se da a un nuevo tipo de conflicto bélico en el cual el adversario no es un ejército organizado a la manera tradicional, con numerosos efectivos repartidos entre generales y soldados, sino a un enemigo configurado en forma de red de células o nodos, activos e independientes entre sí, con capacidad para tomar decisiones propias y realizar acciones de forma unilateral.

El problema que plantean estos nuevos conflictos es que, al no haber, teóricamente, un líder claro, toda baja es sólo un nodo en la red cuya pérdida no pone en riesgo su estabilidad ni genera problemas de liderazgo. El problema ficticio de este tipo de conflictos radica en otorgar espíritu de red difusa a organizaciones que no la tienen, para de ese modo justificar medidas intrusivas que de otra forma no se aceptarían. Un ejemplo sencillo, el término *netwar* se utiliza para definir el tipo de conflicto que representaría al-Qaeda para Occidente en general y para Estados Unidos en particular.

Al-Qaeda, tal como nos la describen a veces los medios de propaganda estadounidense, es un ente oscuro: una red distribuida de terroristas en la cual nadie conoce a nadie, con capacidad autónoma y, en resumen, con todas las características de una organización de este tipo. Este mensaje tiene su lógica en el marco de la política del miedo: un enemigo invisible nunca puede ser derrotado porque nadie lo ve ni antes ni después de una teórica derrota; un enemigo que no puede ser derrotado es un enemigo eterno y las medidas *temporales* implantadas para combatirlo se convierten entonces en intemporales. Si el enemigo contra

el que luchas es una especie de guerrilleros organizados en *cuadrillas* que lo mismo ponen una bomba que usan la red para difundir un mensaje y que no tienen conexión con otras células similares, el estado de excepción en el que estamos sumidos temporalmente en nuestra «lucha contra el terror» no puede dejar de funcionar nunca, ya que no sabemos cuántas de esas células independientes hay con capacidad para actuar porque nadie puede verlas.

Éste es el sencillo argumento que consigue convertir en permanente una renuncia temporal a ciertos derechos, como admitir la traza sin control judicial, el espionaje de nuestras comunicaciones, la videovigilancia masiva o los inacabables controles y restricciones aeroportuarios. Es importante señalar que estas actividades no contribuyen necesariamente a nuestra seguridad: afectan a nuestra privacidad y a nuestros derechos, permiten que estemos más vigilados, pero no tienen por qué contribuir a que estemos más seguros.

La definición de al-Qaeda que la poderosa maquinaria de propaganda estadounidense nos intenta vender (una banda terrorista organizada con líderes claros como Bin Laden, el mulá Omar y dirigentes regionales que

son apresados periódicamente) choca con las medidas que tratan de justificar en nombre de la lucha contra un enemigo serpenteante, difuso y oculto. Existe un doble discurso evidente que se modifica convenientemente. Las evidencias parecen ser más acordes con este último enemigo organizado jerárquica y piramidalmente. Nadie pone en duda el papel que Bin Laden ha desempeñado en esta organización. Hasta se le pudo ver en uno de los vídeos que más circularon en nuestras televisiones en fechas posteriores al 11-S, donde uno de sus lugartenientes se jactaba de haber dado él mismo la orden; esto es, de ser un líder dentro de la organización. ¿Cómo conjugamos todo eso con la idea de células independientes y aisladas que operan ejecutando sus propias acciones aisladas?

A falta de otra información, habrá que pensar que toda organización terrorista posee una cierta organización piramidal y determinados líderes que marcan el camino a seguir. Por tanto, la estructura que hay que combatir no requiere como contramedida la monitorización masiva de la ciudadanía que supuestamente ayudaría a ganar una *netwar*, sino una monitorización centrada en sujetos previamente identificados como sospechosos. Esto ahorraría molestias al

resto de ciudadanos, dinero al erario y aumentaría la seguridad real de nuestra sociedad, además de permitirnos escapar del terror mediático y ayudarnos a vivir sin una psicosis televisiva, callejera y aeroportuaria.

3.3.5. El teatro de seguridad

Llamamos teatro de seguridad al conjunto de medidas de seguridad que, proveyendo sensación de seguridad, no ayudan (o ayudan muy poco) a la mejora de dicha seguridad. El término fue utilizado por primera vez por Bruce Schneier en *Beyond Fear*.[20]

Para actuar realmente como medidas de teatro de seguridad estas medidas deben ser visibles y ser percibidas por todos. De hecho, su misión fundamental es tranquilizar a los ciudadanos haciéndolos creer que se han analizado los asuntos de seguridad y se han tomado las medidas oportunas. Habitualmente, y con el fin ya mencionado de hacer que estén muy presentes, estas medidas interfieren en las actividades normales de los ciudadanos, limitando sus movimientos y sometiéndolos a constantes violaciones de su privacidad.

En la actualidad podemos incluir dentro de este

conjunto de medidas de seguridad la mayoría de controles que se han impuesto con posterioridad a los ataques terroristas del 11-S contra el World Trade Center, sobre todo las restricciones aeroportuarias, que ayudan a aumentar la diferencia entre riesgo percibido y riesgo real.

El problema del teatro de seguridad es que estas medidas tienen un coste sin beneficiar en modo alguno a la seguridad. Este coste puede ser inferior al de las medidas que harían falta realmente, pero al no venir acompañado de una mejora de la seguridad real tiene efectos secundarios bastantes graves. El continuo desfile de militares armados en aeropuertos y estaciones de tren de las principales capitales es un ejemplo de ello. Infunden miedo a la población al hacerla creer que así está más segura, cuando la presencia militar no va a disuadir a un terrorista suicida. El motivo por el que se recurre a la creación de miedo es que de otra forma las medidas serían rechazadas. En el teatro de seguridad, la política del miedo y la doctrina del shock se dan la mano. Está claro que sería mucho más beneficioso educar a la población para que aceptara el peligro y reaccionara adecuadamente ante determinadas situaciones de riesgo, pero eso requiere tiempo y dinero público. Al final

se opta por la opción barata y coercitiva: el teatro.

3.4. La sociedad digital y la vigilancia

A lo largo de los dos últimos siglos todo avance tecnológico ha sido puesto al servicio de las herramientas de control estatal y de la vigilancia de sus ciudadanos. La situación actual no es algo nuevo si consideramos que el telégrafo permitió que los policías se comunicasen entre sí y enviasen mensajes de unas oficinas a otras para solicitar información o apoyos. Lo que sucede es que en los últimos años la tecnología está avanzando a una velocidad que aumenta de forma exponencial, siendo el número de nuevas herramientas disponibles cada vez más elevado y siendo mayor el poder de cómputo, análisis y almacenamiento informático de éstas.

Esta situación, unida al desarrollo de la sociedad en red, permite almacenar una gran información sobre las personas y comunicarnos desde un entorno local con un entorno lejano sin desplazarnos y en un tiempo reducido. De esta forma, se cotejan informaciones referentes a un determinado individuo o se añade nueva información a las bases de datos que estará disponible en próximas consultas,

desde donde quiera que éstas se realicen.

Aquí es donde la política del miedo que hemos comentado anteriormente comienza a jugar un papel importante. La extensión de la videovigilancia ciudadana en nuestras calles y nuestras redes de metro, la retención de datos de telecomunicaciones, la intercepción y violación del derecho al secreto de las comunicaciones y las nuevas restricciones en los aeropuertos son medidas políticas, decisiones políticas que atentan contra nuestros derechos fundamentales y nos sitúan bajo la lupa constantemente.

En el contexto actual, donde cada vez más queda un registro de todas nuestras actividades en alguna parte (algo que será aún más inevitable con la migración de la telefonía convencional a la telefonía digital y a la telefonía sobre IP), esto supone un paso más hacia la muerte de la conversación efímera, ésa cuyas palabras se llevaba el viento. La idea es constituir un panóptico estatal omnipresente y coercitivo; un sistema perfectamente vigilado donde todo es, en todo momento, controlado por los vigilantes. Cuídese de decir algo de lo que más adelante pueda arrepentirse porque, no lo dude, alguien lo tendrá grabado y, conociendo al género humano, puede dar por seguro que, si hiciera falta, se usará

en su contra.

Esta nueva conducta tiene consecuencias en nuestras aspiraciones si nuestros opositores tienen acceso a nuestros datos o los de nuestras comunicaciones. Esto, que a la mayoría de las personas nos puede parecer algo lejano, cobra verdaderos visos de realidad cuando se trata de la privacidad de personalidades políticas, que pueden ver arruinada su reputación por escándalos en su vida privada que poco tienen que ver con su capacidad como gestor público. Es lo que le sucedió a Mark Foley, ex senador conservador de Estados Unidos, en fechas previas a la cita electoral de su país en 2006.[21] Estos actos oportunistas conllevan una pérdida de calidad democrática y podrían generalizarse con la extensión del registro de datos recogidos sobre todos nosotros gracias a las telecomunicaciones, la videovigilancia y tecnologías como la RFID.

3.4.1. El panóptico de Jeremy Bentham

Si hay alguien a quien se puede considerar el padre de la vigilancia moderna ése es sin duda el británico Jeremy Bentham, quien a finales del siglo XVIII diseñó la que, según

él, era la cárcel perfecta y a la que denominó *panóptico*, debido a su diseño especial.[22] El panóptico es un sistema carcelario dotado de un sistema de vigilancia coercitiva que no pretende penalizar las malas acciones, sino que está concebido para evitarlas. Este sistema busca amenazar al sujeto, convencerlo de que cualquier acción indebida será advertida por el vigilante (principalmente el Estado) y de que la represalia será tan desproporcionada que no vale la pena siquiera intentarlo.

Su nombre, mezcla de dos raíces griegas (*pan-* que significa «todo» y *-optikós* que significa «visión») evoca una cárcel en la que se vigilaría todo. En el diseño de Bentham esto se haría desde un único punto y sin que el vigilante fuera visto en ningún momento. Según la teoría de vigilancia de Jeremy Bentham, bastaría la certeza de la vigilancia misma para que cada uno, sintiéndola pesar sobre sí, la interiorizara y comenzara a vigilarse a sí mismo, eliminando las acciones no permitidas para, de este modo, eludir los castigos. Evidentemente, el problema del panóptico, la consciencia y el condicionamiento de nuestra conducta al estar vigilado, es aplicable a toda tecnología de control. No por ello hay que dejar de indicar que es en el

ámbito de la vigilancia visual, precursora de baja tecnología de la actual videovigilancia, donde surge este concepto represivo.

Bentham se dio cuenta de que este panóptico era un gran invento, útil no sólo para una cárcel, sino también para las fábricas, donde se podía coaccionar a los obreros que pudieran estar tentados a trabajar menos de lo debido. Si bien el modelo de Bentham fue criticado, se impuso aplastantemente y esta idea fue adoptada ya en el diseño de las primeras cárceles construidas por la recién triunfante República Francesa.

El panóptico en la actualidad

Aunque parezca un tanto extraño, éste es el principio que desde finales del siglo XVIII rige todas las cárceles, escuelas y fábricas construidas en Occidente desde entonces. El panóptico es una suerte de política del miedo dieciochesca que no sólo ha logrado sobrevivir hasta nuestra época, sino que se ha fortalecido con el paso del tiempo.

En la actualidad, el mito del panóptico sigue presente y se fortalece con la incorporación de nuevas tecnologías a los cuerpos policiales. Está claro cuál es el

motivo: el control. Es evidente que tanto en las cárceles como en las fábricas esta idea ha arraigado por motivos tan diferentes como similares y, en ambos ambientes, la idea de que un superior o un carcelero te amonestará si te descubre haciendo algo incorrecto está interiorizada por todos. El ideal de policía panóptica, extendida a numerosos ámbitos, es la herramienta utilizada para mantener el orden público y, sin duda, empleada con mesura ha permitido el desarrollo de las democracias contemporáneas. Pero, ¿qué sucede si este control sobrepasa los límites?

El principal problema es que una sociedad excesivamente vigilada jamás podrá ser libre. La conciencia de que estamos siendo vigilados y de que toda acción que llevemos a cabo será conocida por instancias superiores (sociales, laborales, policiales) nos condiciona en nuestros actos. Pregúntese a sí mismo, ¿qué pensaría si cualquiera pudiera verle tal y como se despierta por las mañanas, sin vestir, peinar ni duchar? ¿No le gustaría poder controlar a partir de qué momento pueden verle las personas que le rodean? La vigilancia y la excesiva exposición pública condicionan las cosas que decimos y el modo en que las decimos, las cosas que hacemos y la contundencia con que

las hacemos. Y no afecta sólo nuestro ámbito más íntimo, ya que la conciencia de las represalias que seguirán al descubrimiento de cualquier acción punible es un arma poderosa para impedir que se lleven a cabo justamente muchas de esas acciones, aunque muchas de ellas pudieran estar justificadas y ser justas. Ésa es la línea que separa la vigilancia tolerable del exceso de control: a veces está tan difuminada y tenemos el control tan asumido, que se sobrepasa sin que la sociedad proteste por estas violaciones.

Vigilar y castigar

La visión del panóptico desarrollada por Bentham es todo un referente en la prevención de conductas no deseadas mediante la coerción. Sin embargo, si hay alguien que haya analizado con detalle ese modelo panóptico y su aplicación en la sociedad actual ése es Michel Foucault en *Vigilar y castigar*, su obra de 1975.

En su obra, Foucault analiza el cambio radical sufrido en las metodologías de castigo, que él llamó *tecnologías de castigo,* durante la época de la revolución francesa. Así, en menos de un siglo se pasa de la ejecución pública, o castigo monárquico, a las prisiones actuales,

basadas en el ideario panóptico de Bentham, o castigo disciplinario. De este modo, el oscuro calabozo de las prisiones anteriores a la revolución francesa se sustituye por una cárcel luminosa y brillante en la cual la visibilidad es una trampa, ya que favorece la labor del vigilante.

Para Foucault los conceptos de conocimiento y poder están tan entrelazados, que a menudo son inseparables, por lo que percibe la forma en que la sociedad actual está organizada como una evidencia de que todo, desde las cárceles hasta los trabajadores sociales y desde la policía hasta los maestros, está sujeto a una misma forma de poder: el que otorga el conocimiento-poder obtenido mediante la vigilancia que hemos heredado del modelo de Bentham.

3.4.2. Sociedad digital bajo vigilancia: la sociedad de control

El binomio sociedad digital y vigilancia hacen posible el tránsito a la sociedad de control, entendiendo como tal una sociedad no asamblearia como la actual, sino una sociedad totalitaria en la que un reducido número de personas impone medidas y conductas al resto y en la que esta imposición es posible debido a un estricto control de lo

que los ciudadanos pueden hacer de forma individual.

La sociedad de control es el sistema social pensado para sustituir a las democracias dieciochescas y su asamblearismo. Está basada en las posibilidades tecnológicas abiertas con los desarrollos de la segunda mitad del siglo XX y tiene su principal apoyo en la deliberada ausencia de medidas legales que limiten el abuso de estas tecnologías. Para entender bien lo que es la sociedad de control primero hay que detenerse a describir el mundo en que vivimos: la sociedad parlamentaria o asamblearia.

La sociedad parlamentaria

La sociedad parlamentaria ideal se caracteriza por la separación de poderes (legislativo, ejecutivo y judicial) y porque el pueblo elige democráticamente un número de representantes sobre los que recae la responsabilidad y el poder de dirigir la vida pública (leyes, medidas económicas, gobierno). Cada cierto tiempo, la población elige nuevos representantes, momento en el que -idealmente- aquellos representantes que han actuado mal (por incapacidad o por corrupción) son reemplazados por otros. El sistema puede tener sus deficiencias, como el que minorías muy pequeñas

jamás vean materializadas sus propuestas, pero en general no es un sistema aborrecible: al menos es la mayoría del pueblo la que elige a los dirigentes.

¿Cuál es el problema? Nuestra sociedad parlamentaria está siendo debilitada por las élites sobre las que repetidamente recae el poder. El método escogido ha sido el de crear instituciones supranacionales carentes de todo carácter democrático. Estas instituciones están encarnadas tanto en estados macroestatales (como la UE y todas sus instituciones) como en instituciones internacionales como el FMI (Fondo Monetario Internacional), el BM (Banco Mundial), la OMC (Organización Mundial del Comercio), la ONU (Organización de las Naciones Unidas). Todas ellas adolecen de un serio déficit democrático. Esta doctrina se conoce como Consenso de Washington y persigue apartar a los ciudadanos del poder, aunque para ello haya que mentir e imponer una doctrina de libre mercado de agrio autoritarismo, a la que se recurre para desmantelar los servicios públicos y debilitar la influencia de las instituciones básicas de la democracia. Las partes implicadas en este proceso de transformación incluyen al poder político (que encarna el gobierno) y al

poder económico (que encarnan las empresas). En España se han sumado además los sindicatos, bajo estricto control político, algo que recuerda alarmantemente aquel corporativismo añorado por Mussolini. Según el propio modelo de Estado del dictador italiano: «El corporativismo se refiere a un estado policial gobernado bajo una alianza de las tres mayores fuentes de poder de una sociedad -el gobierno, las empresas, y los sindicatos-, todos ellos colaborando para subyugar a la población y mantener el orden en nombre del nacionalismo».

De la sociedad parlamentaria a la sociedad de control

La sociedad digital en la que vivimos hace que para mantener el orden se deba recurrir a un férreo control de los ciudadanos. La sociedad digital, participativa y libre, se convierte entonces en la sociedad de control. De la amplia libertad de creación y comunicación que permite la tecnología digital pasamos a la vigilancia extensiva de los ciudadanos, que es posible gracias a esa misma tecnología digital. De la libertad de creación, uso y transmisión de información y conocimiento pasamos al levantamiento de vallas virtuales y la creación de propiedades allá donde sólo había algo que nos pertenecía a todos para servir a los

mismos intereses económicos y políticos mencionados anteriormente mediante el *cercamiento digital*[23] y la generación de escasez artificial.

Así, la tecnología, que nunca es neutral, se convierte en la llave que puede hacer que nuestra sociedad sea más libre, pero también convertirla en una desagradable distopía que utiliza el ideario heredado del panóptico de Bentham como forma de control. En este caso, la coerción panóptica se fortalece mediante la dotación de los cuerpos policiales con todo tipo de herramientas tecnológicas y de vigilancia. No debemos olvidar que parte de su función, mantener el orden, la llevan a cabo no gracias a las armas, sino a la evocación de su naturaleza panóptica que todo lo vigila: la conciencia de que, si haces algo malo, la policía lo sabrá y serás culpado por ello.[24]

La clave está en el uso que se hace de la tecnología, en cómo se articulan su regulación y sus posibilidades. El problema viene definido por dos topes: el inferior (dónde se limita el control que se puede hacer de las mismas) y el superior (hasta dónde se permite su libre uso). Lo habitual en lo referente a tecnologías y a su uso es que se legisle de forma ultrarrestrictiva para nuestros derechos, o bien que

no se legisle en absoluto -para verlas venir con tiempo- a fin de permitir abusos que otras leyes como la LOPD no permitirían. En muy pocas ocasiones se tiene la posibilidad de ver una reforma legal que salvaguarde nuestros derechos adecuadamente. Para justificar estas reformas en contra de nuestros derechos se recurre al nacionalismo corporativista, como ya hemos dicho. Éste puede encarnarse de dos formas:

- La seguridad nacional: las medidas se toman para defender la nación, amenazada por el uso que hacen de la tecnología enemigos difusos a los que nadie puede ver. El clásico argumento de *netwars* esgrimido en la época de la guerra fría y «supuestamente» instigado desde Moscú. El mismo argumento utilizado por George Bush tras el 11-S en su guerra contra el terror: «Es un enemigo difuso y la guerra será larga».

- La economía nacional: las medidas se toman para proteger la economía de la nación, amenazada por el uso que los ciudadanos de a pie hacen de la tecnología.

Esto significa que el enemigo de los Estados está tanto dentro como fuera de su territorio. Nadie se

sorprenderá de que el Estado vea enemigos fuera de su territorio, y por eso la conclusión más llamativa del análisis anterior es que los Estados construyen su discurso pensando que hay un enemigo interior al que combatir. Esto es sorprendente en un primer momento, pero no tanto si consideramos que en las grandes sociedades bajo vigilancia del siglo XX ya sucedió así. Para defenderse de este enemigo difuso cualquier medida de control estará justificada (espiar las comunicaciones, videovigilancia extensiva, control aeroportuario, vigilancia y control de la red, obligar a utilizar tarjetas de identidad para cada vez más acciones). La sociedad de control no es, por tanto, sino una tecnocracia autoritaria: tecnoimperialismo sin vergüenzas.

La sociedad de control es la sociedad nacida de la política del miedo. Es importante no perder esto de vista, ya que nos ayudará a entender los motivos por los que se está organizando de esta forma. En un ecosistema distribuido y con facilidad extrema para la información y la comunicación, tras numerosas promesas incumplidas, los partidos políticos habían perdido su influencia. La sociedad de control tiene como objetivo permitir a los partidos políticos recuperar la influencia social perdida, para así

poder gobernar y legislar, dirigir la vida pública y nuestra economía sin que nadie cuestione sus actos. Los partidos políticos pretenden recuperar, mediante la recurrencia a un nacionalismo rampante, la influencia perdida tras décadas de desilusiones electorales y promesas incumplidas. Con esta recobrada influencia intentarán aprobar todo tipo de medidas económicas y de restricción de libertades que de otra forma no podrían implementar.

Vale la pena indicar que, casualmente, estos nuevos bríos nacionalistas se ven potenciados por las políticas impositoras supranacionales del Consenso de Washington, que provocan una percepción fría y lejana de las instituciones de gobierno actuales y sus formas, incitando a muchas personas a oponerse a este nuevo orden haciendo suyos esos argumentos nacionalistas, que se perciben más cercanos, en lo que es una respuesta equivocada a este fenómeno de reorganización supranacional, ya que la oligarquía encargada de alejar a la ciudadanía del poder es la misma (ya hemos hablado de *la alianza del corporativismo*) que promueve el renacimiento del nacionalismo que entorpece la reacción social y facilita la extensión de estas nuevas medidas de gobierno y control.

Asimismo, mediante este control pretenden recuperar el poder que las nuevas tecnologías de la información les han arrebatado. No hay que pasar por alto en este análisis que toda arquitectura de la información sostiene una arquitectura de poder. La arquitectura de la información ha sido históricamente piramidal y centralizada en los poderes político y económico; las nuevas tecnologías abren la posibilidad de articular debates, problemas y soluciones al margen de estos poderes y, por tanto, la arquitectura de poder subyacente se tambalea.

Dicho de otra forma, Internet y las actividades en red en general arrebatan a los viejos poderes su capacidad de definir los temas y las preocupaciones de la gente, la agenda pública, haciendo que los partidos políticos pierdan su papel de dirección y timón social. Los partidos políticos han perdido su *leitmotiv* porque la gente ha dejado de buscarlos como solución, por eso el desapego social a los mismos es creciente. Las personas han comenzado a buscar a las personas. Es por eso que, cuando se trata de regular y salvaguardar estas nuevas libertades adquiridas, todos ellos actúan rechazándolas, sin importar los enfrentamientos ni las ideas que los puedan separar en otros asuntos. Frente al

sistema distribuido que resta poder a todos los partidos, éstos escogen la alianza de su club cerrado para doblegar al nuevo mundo: quieren seguir siendo el nodo por el que todo debe pasar y la nueva sociedad digital les aterra porque dejan de hacer falta en el mapa social. Por eso la rechazan, por eso les da miedo. Es por ello que cuando se trata de proteger derechos digitales, la clase política se une en contra de la sociedad, a menudo para proteger los intereses del poder político, pero también para proteger los derechos de los importantes oligopolios económicos que, gracias a la oleada de privatizaciones realizadas en las últimas tres décadas, poseen casi todas las industrias críticas (energéticas, telecomunicaciones) y apoyan económicamente a estos partidos para, en parte, pasar inadvertidos a los ojos de la sociedad y escapar a sus iras.

La sociedad de control presenta, en consecuencia, muchos problemas, y el primero de ellos es su gran déficit democrático. La sociedad de control se sustenta en el poder coercitivo de la vigilancia y necesita dichas imposiciones coercitivas para subsistir. Allí donde la sociedad parlamentaria y asamblearia posee protocolos en los que todas las partes llegan a un acuerdo (unas elecciones

democráticas son un protocolo de gobierno), la sociedad de control tiene controles, y un control es siempre una imposición de una parte a la otra (como la imposibilidad de mantener la intimidad de tus comunicaciones). La sociedad de control es incapaz de defender la democracia porque no nace de ideales democráticos, sino impositivos, y por ello, para evitarla, es necesaria la interposición de protocolos, acuerdos sociales que limiten estas acciones y mantengan nuestra sociedad dentro de los límites que requiere toda sociedad libre.

3.5. La guerra contra el terror como alienante

Desde que los medios de comunicación aparecieron y demostraron su poder para influir en la agenda pública, los gobiernos se han empeñado en mantener un cierto control de los mismos para que éstos presten mayor atención a lo que ellos consideran importante y enfoquen la comunicación del modo que consideran conveniente. Lo han hecho siempre, aunque ello significase desatender las inquietudes de la gente o no ser fieles a la verdad.

Los medios de comunicación amplifican hasta los

límites las informaciones sobre «la guerra contra el terror». En estos mensajes nuestros gobernantes nos dicen que la guerra contra el terror se está ganando, que al-Qaeda ya no es tan poderosa como antes y que la victoria final es inevitable. Acto seguido, y descuido contradictorio, nos vuelven a recordar que al-Qaeda es una organización extremadamente peligrosa, con miles de tentáculos repartidos por todo el mundo que se han fortalecido tras la guerra de Irak, y que se necesita todo nuestro esfuerzo y colaboración para derrotarla, incluso si esta colaboración implica renunciar a algunas libertades fundamentales, como el secreto de las comunicaciones, e incluso si esta colaboración incluye destinar a la guerra contra el terror el dinero que se debería dedicar a mejorar las formación de nuestros jóvenes o el cuidado de nuestros mayores.

El poder alienante de la política del miedo tiene repercusiones en nuestra privacidad. La política del miedo se emplea para conseguir que el pueblo acepte medidas que de otra forma no aceptaría. Con ello se consigue que pasen por excepcionales y temporales medidas altamente impopulares de duración indefinida que amenazan con ser permanentes. ¿O acaso alguien piensa que, en caso de que la

guerra contra el terror deje de formar parte del discurso de la seguridad, se van a reducir drásticamente los controles de seguridad en los aeropuertos o la videovigilancia ciudadana? No ocurrirá, porque no son medidas temporales aunque para convencernos de su necesidad hayan recurrido a amenazas puntuales y promesas de temporalidad.

3.5.1. Lo que los terroristas quieren

Utilizar la guerra contra el terror, islamista o independentista, como excusa para recortar las libertades civiles tiene una doble consecuencia negativa. La primera y básica es que los terroristas estarían encantados si de repente nuestras libertades básicas se vieran reducidas y ninguneadas. Si súbitamente un día no viviésemos en una sociedad libre, sino en una sociedad aterrorizada y autoritaria, los terroristas habrían tenido éxito. Si de pronto nuestras vidas no pudieran desarrollarse en libertad, el objetivo básico de los terroristas se habría cumplido: habrían derrocado nuestra libertad. Además, ese entorno facilita la inaceptable justificación de la violencia: los actos terroristas estarían justificados como forma de oposición violenta a un régimen que nos aprisiona.

Hay que tener en cuenta que el objetivo último de los terroristas es sembrar terror, a veces porque pretenden conseguir un objetivo político más adelante, a veces como simple consecuencia del odio. Los muertos que provocan los terroristas, por triste y doloroso que parezca, no son el objetivo, sino el medio. Reventar aviones, trenes, mercados, quemar autobuses o cajeros, los actos de terrorismo no son el fin, son la herramienta.

El objetivo real de los terroristas es el resto de la población; millones de personas que no somos asesinadas, sino aterrorizadas por los asesinatos de personas con las que nos identificamos: ciudadanos libres como nosotros. El objetivo real del terrorismo no es matar o destruir coches o inmuebles, sino el acto mismo de aterrorizar. Y el éxito del terrorismo depende, siguiendo esta lógica, no de que sus acciones programadas lleguen a materializarse, sino de nuestra reacción frente a las mismas.

Por eso utilizar el terrorismo como alienante es contraproducente. Y nuestros dirigentes, con sus políticas del miedo dirigidas a recordarnos que vivimos en un mundo lleno de peligros donde cualquiera puede activar el detonador que acabará con la vida de nuestros hijos o con

nuestra propia vida, están haciendo exactamente lo que los terroristas quieren: aterrorizarnos para conseguir que obedezcamos.

Lo que habría que analizar es qué ganan las instituciones públicas con ello. Aquí está la paradoja: nuestros gobiernos reducen nuestras libertades y nuestros derechos para defendernos, a todos nosotros y al Estado, de unos terroristas que quieren acabar con nuestras libertades y nuestros derechos. ¿No resulta paradójico, entonces, que se produzca ese recorte de libertades? En la lucha contra el terror, George Bush ha llegado a afirmar que la tortura, como el ahogamiento simulado o *waterboarding*, está justificada para defender a Estados Unidos.[25]

Antes de que alguien se pregunte si estoy equiparando la muerte de un inocente con las molestias que genera el teatro de seguridad y las colas en el aeropuerto, los sistemas de videovigilancia públicos que inundan nuestras ciudades y el hecho irritante de que todo, absolutamente todo, lo que hacen sea *por nuestra seguridad* frente al terrorismo, debo decir que no las estoy igualando. Ni muchísimo menos. Sólo quiero recalcar la contradicción que supone combatir el terrorismo con el terror, terror

mediático en este caso. La privacidad es un derecho fundamental que, sin el más elemental derecho a la vida, no sirve absolutamente para nada, pero eso no impide que la privacidad siga siendo un derecho fundamental a preservar, porque en ausencia de privacidad la vida de las personas corre peligro.

La realidad es tan desagradable que parece indicar que los más radicales de cada bando podrían brindar para celebrar cada endurecimiento de esta pugna, ya que cada uno de ellos tiene, a su modo, una posición de fuerza en su entorno. La supervivencia del clan está asegurada por encima de lo que podría ser el interés general, un interés general que se ignora cuando es el terror policial el que causa los muertos, como en el caso de Jean Charles de Menezes, que murió en 2005 cuando le disparó la policía mientras leía el periódico en un vagón de metro, o el de Carlo Giuliani, muerto a manos de la policía durante una manifestación de repulsa al G8 en Italia en 2001.

3.5.2. La vigilancia como vía de perpetuación

Si unimos el poder del terror para conseguir que medidas impopulares sean aceptadas al teatro de seguridad

incapaz de impedir un atentado, la última justificación que tenemos para que desde algunos gobiernos se apueste por sistemas de vigilancia global en lugar de sistemas de vigilancia de sujetos sospechosos es que en algún momento podrían necesitar datos de cualquiera para impedir que lleve a cabo alguna protesta legítima (pero en contra de los intereses del poder establecido) o quizá para destruir su reputación, en el caso de ser oposición política.

Ambos casos apuntan a un mismo fin: utilizar la vigilancia para perpetuarse en el poder más allá de lo que permitiría la democracia. No estoy diciendo, ni mucho menos, que estemos viviendo en alguno de nuestros cuentos distópicos en los que las mayores catástrofes son causadas por el gobierno mismo para perpetuarse. No estoy diciendo que la situación esté tan deteriorada que la única forma de cambiar las cosas sea mediante la anarquía, rebelión, máscaras y asesinatos, como propone Alan Moore en *V de Vendetta*. Pero debemos ser conscientes de dónde y cómo nos encontramos ahora para identificar adecuadamente la encrucijada de la que debemos salir.

En el contexto de la sociedad digital, donde la red se utiliza para todo, donde existe un almacenamiento masivo

de datos de comunicaciones por parte del Estado y donde cada receptor de un mensaje, por pequeño que éste sea, tiene la posibilidad de guardar una copia del mismo, la conversación efímera consistente en hablar y olvidar está en vías de extinción. ¿Se podría abusar del acceso a esta información para desestabilizar la imagen de un contrincante político? Sí, incluso se podría disfrazar de filtración casual lo que podría ser una estudiada operación de descrédito.

3.5.3. La guerra como negocio

Resulta evidente, años después de los atentados del 11-S en Nueva York, que tras la conmoción inicial se ha aprovechado la coyuntura para llevar a cabo una de las operaciones económicas más grandes de nuestro tiempo. Sin duda se trata de un gran negocio, que en Estados Unidos ha incluido, por primera vez en las democracias modernas, la privatización y subcontratación de un sector tan importante para la seguridad de los países como es la defensa: la privatización de la guerra.

Cuando hablo de la privatización de la guerra no me refiero únicamente a la privatización del ejército llevada a

cabo por George Bush y su contratación de mercenarios para mantener la ocupación de Irak (algo que ya sería suficientemente grave), sino al uso mercantilista de la guerra contra el terror. En este sentido, es imposible no mencionar el endurecimiento de las medidas de control antiterrorista que se produjo en Estados Unidos en agosto de 2007. Estas medidas contemplan que se destinen más fondos públicos a aquellas ciudades en las que haya más indicios de posibles atentados terroristas;[26] han leído bien: indicios. Esta ley, que aparentemente parece una buena idea, podría acabar desbocando el uso de la política del miedo, ya que cuanto más creíble sea la amenaza que se cierna sobre una ciudad, más fondos recibirá del erario público. Así, aquellas que sean capaces de crear los miedos más oscuros, recibirán más fondos públicos, para desesperación de sus ciudadanos.

3.6. El rediseño del contrato social

Muchos de nosotros tenemos la suerte de no haber vivido bajo una dictadura. Entre nuestras obligaciones se cuenta la de de no descuidar algo tan importante como permitir a los que nazcan después disfrutar de esta posibilidad: nacer y vivir en democracia. Para ello hay que proteger el contrato social actual.

En las democracias actuales el contrato social se puede resumir, a grandes rasgos, como un contrato por el que los ciudadanos pagamos unos impuestos para dotarnos de un gobierno, unas instituciones y unos servicios públicos que nos pertenecen a todos. Sin detrimento de estos servicios públicos, todo aquel que quiera puede poner en marcha sus propios servicios, formar su propio negocio y hacer de él su modo de vida. Nada está prohibido en el mar de posibilidades disponibles.

En los últimos tiempos muchos líderes europeos plantean la necesidad de rediseñar el contrato social añadiendo a la ecuación del mismo una cantidad de parámetros cuya valoración no es viable sin una fuerte vigilancia de los ciudadanos. Es el caso del ya ex primer ministro británico Tony Blair, que proponía adaptar el contrato social para obligar a aquellos que son más propensos a tener enfermedades a llevar una dieta sana y pagar por ser atendidos en una sanidad pública que ya están pagando con sus impuestos.[27]

Esto último resulta bastante insolidario, porque los impuestos sirven precisamente para redistribuir la riqueza y las oportunidades entre aquellos que, por algún motivo, se

ven obligados a afrontar costosos tratamientos médicos o molestas enfermedades; también en el caso de los enfermos de obesidad. E incluso podríamos añadir un agravante, ya que en muchos casos las personas se ven obligadas a trabajar lejos de su hogar, a comer fuera de casa o a pasar gran cantidad de tiempo fuera del hogar. En este caso una persona podría no llevar una dieta sana sin que fuera estrictamente culpa suya, sino del propio sistema laboral contemporáneo que nos empuja a una movilidad constante. Todavía es mucho más interesante revisar la hipótesis de partida (ciudadanos que genéticamente son más propensos a engordar) y el primer punto propuesto por Blair: que sean obligados a llevar vida sana o paguen más impuestos si no se someten a esta dieta. Esto es algo que ya se ha aprobado en otros países europeos como Finlandia.[28]

Aunque Blair, que ha transformado Reino Unido en la sociedad occidental más vigilada,[29] ya no es primer ministro del país, el cargo lo ha heredado quien desde un principio fue su hombre de confianza, Gordon Brown. Mucha sorpresa sería que las ideas de Brown fueran muy diferentes a las presentadas por Tony Blair, y los primeros meses de su gestión son una continuación de la senda de

vigilancia extensiva y recorte de derechos que abrió Blair. Además, desde mayo de 2007 los partidarios de reformar el contrato social tienen a un nuevo paladín en la figura del conservador Nicolas Sarkozy, presidente de la República Francesa, quien en los días posteriores a su elección declaró que es urgente reescribir el contrato social.[30]

3.6.1. La amenaza del rediseño del contrato social

Existen serios indicios de que en los últimos tiempos se pretende romper el estado de equilibrio de nuestro contrato social, de forma que muchos de aquellos derechos conseguidos con mucho esfuerzo se renegocien a la baja o incluso suprimidos. En el contexto de la extensión globalizante del Consenso de Washington y la privatización y subcontratación de la mayoría de los servicios públicos, los Estados aparecen como muñecos de trapo debilitados incapaces de forzar a las grandes corporaciones transnacionales. Esto propicia que las grandes multinacionales no tengan dificultad para cambiar de nacionalidad de un día para otro, llevándose a sus trabajadores a países del tercer mundo donde, por arte y magia de la ósmosis que inducen las políticas

antimigratorias, los sueldos son enormemente inferiores.

Como consecuencia de estos flujos de trabajo y de dinero (que no de trabajadores) promovidos desde la oligarquía económica y política mediante esta falsa globalización, los trabajadores del primer mundo ya no están vinculados directamente a la producción de los bienes que consumen y ello debilita la posición de fuerza que podrían mantener en una nueva negociación del contrato social. Si la teoría dice que antes de sentarse a negociar hay que asegurarse una posición de fuerza, la experiencia nos dice que renegociar un contrato social ahora es una mala idea.

Como frenar completamente estas medidas no es sencillo, los derechos van menguando (pensiones, prestaciones por desempleo, libertades civiles). Para ver hasta dónde podemos llegar, imagine lo que sería un espejo de la tristemente famosa directiva Bolkestein,[31] en la que los derechos laborales de los países desarrollados no se igualaran ya a los del país más pobre de la UE (algo ciertamente preocupante y que fue lo que promovió campañas ciudadanas contra esta directiva),[32] sino a los de cualquier país asfixiado económicamente del sudeste

asiático.

Visto el desamparo en el que los sectores más desfavorecidos de la sociedad se encuentran frente al ideario de estos reformistas y vista la poca presión que se puede ejercer desde el sector terciario mayoritario en nuestra economía sobre un Estado cada vez más débil, acceder a la revisión de nuestro contrato social en nombre de una viabilidad económica que las grandes empresas dicen necesitar equivaldría a un suicidio social. La mayoría de las veces estas empresas ni siquiera tienen déficit, sino que argumentan que sus beneficios no son tan abultados como en años anteriores. Pero son beneficios al fin y al cabo, por lo que ¿justifican estas quejas el rediseño del contrato social?

3.7. Tolerancia hacia la vigilancia

La lucha contra la sociedad de control no es una lucha a corto plazo; de hecho, podría decirse que es la lucha eterna (imposición de control contra resistencia antidisciplinaria), pero sí es una lucha que se endurece con el paso del tiempo. En la lucha contra la sociedad de control el tiempo juega en nuestra contra. El desarrollo de

tolerancia, entendida como capacidad de soportar estas medidas sin que nazca una sensación de desasosiego y rechazo de las mismas, es un factor dependiente del tiempo y que aumenta exponencialmente con el paso del mismo.

El hecho de que el tiempo sea nuestro enemigo se debe a que éste favorece el desarrollo de tolerancia hacia las medidas de control. Con el paso del tiempo interiorizamos la existencia de controles que nos limitan, condicionan y adoctrinan. El proceso en sí de interiorizar el control ataca y debilita la oposición al mismo, pues sería como atacarnos a nosotros mismos. No desarrollamos tolerancia a la idea de estar controlados, ya que a nadie le gusta sentirse controlado, sino que dejamos de percibir el control como tal, creándose un desajuste entre el control real al que estamos sometidos y el control percibido. Este desajuste entre lo real y lo percibido hace que no seamos plenamente conscientes de hasta qué punto existen controles y todo está vigilado, lo que reduce toda posibilidad de oposición a esta vigilancia.

El discurso sobre el que se construye este control en un mundo de redes está encaminado a enlazar directamente las medidas de control con la capacidad de gobierno de la sociedad actual. Los mensajes de la política del miedo y la

guerra contra el terror persiguen crear un imaginario en el que un mundo distribuido no es gobernable en términos de promesas y de un futuro mejor, sino que la gobernabilidad misma pasa a estar definida en términos de seguridad, aunque en ningún momento se aclara si estas medidas protegen a los ciudadanos o a los poderes establecidos del ataque (que podría darse en forma de simple indiferencia y búsqueda de realidades de organización alternativas) por parte de esos mismos ciudadanos. Que la construcción misma de estas medidas y el modo en que se comunican al público constituye otra forma de control y manipulación social es algo evidente, aunque no lo abordaremos en este capítulo.

En ese sentido, también la manera en que se construyen estos discursos, apelando al civismo y al patriotismo para favorecer esta asimilación, debe ser lo primero en recibir nuestras críticas, pues es con la ayuda de estos discursos con lo que se logra que toda oposición, crítica y propuesta de reforma sea rechazada y marginada. De repente, a alguien que se opone a las medidas de control se le percibe como un cómplice de los delincuentes o un *odioso antipatriota*. Es el discurso el principal vehículo para la

asimilación de estas medidas y para el desarrollo de tolerancia al control. No podemos dejar de considerar que las medidas de control forman parte de la educación y el condicionamiento que las generaciones posteriores deben recibir para garantizar la continuidad del sistema, como parte de una violencia simbólica[33] que diluya sus protestas hasta volverlas inofensivas.

El desarrollo de tolerancia a las medidas de control comienza a operar tan pronto éstas están operativas, ya que a la inclusión de las mismas en nuestros hábitos (con la consecuente reducción de atención prestada, pues abrir la puerta con el transpondedor pasa a ser un acto mecánico y no un acto razonado) hay que unir que, debido al modo en que se justifican las mismas, muchas personas son automática e inconscientemente obligadas a aceptarlas. Sin embargo, en nadie es esta tolerancia tan acentuada como en las generaciones que nacen y crecen con posterioridad a la entrada en vigor de las mismas. Aquello que estamos acostumbrados a utilizar desde niños nos resulta más fácil de comprender, y aquello que entendemos con facilidad nos da confianza. El proceso de asimilación de las medidas por parte de los jóvenes constituye un enorme factor en contra

de la resistencia a estas restricciones y controles, y por eso la oposición a las medidas de control es una lucha que, sin constituir una derrota asegurada a largo plazo, será más fácil ganar si evitamos que este nuevo régimen se prolongue innecesariamente en el tiempo.

4. Tecnologías de control

Conocemos como tecnologías de control todos aquellos desarrollos tecnológicos que ofrecen importantes aplicaciones en el ámbito de la vigilancia y el control. Estas tecnologías se pueden utilizar en muchos ámbitos y no en todos los casos serán realmente preocupantes, pero nos centraremos en la vigilancia de personas para ejercer control. Este control puede referirse tanto al control de personas como al control de flujos de información. En ambos casos el modo en que las personas interactúan con su entorno social se ve modificado y limitado.

4.1. Control

Dentro de las posibilidades que confiere el control

movimientos o actividades. Por supuesto, el control de la información permite controlar a las personas en último término y el control de las personas también permitirá regular la información. Todo estaría controlado, al existir una relación de causalidad entre el control de un ámbito y su derivada en el otro. De esta forma, distinguiremos el control de las personas o el control de la información en función del nivel al que tiene lugar la intercepción de la información y el control del sistema.

4.1.1. De la información

El control de la información ha constituido desde siempre una de las herramientas básicas del poder. Con la aparición de la imprenta, en sólo unas décadas la iglesia perdió el monopolio de producción literaria que había tenido hasta entonces (heredado del sistema medieval, donde el control era absoluto). En esas décadas se multiplicó el número de personas con capacidad para producir libros, de forma que aunque el clero continuó teniendo un gran control del ecosistema de la información éste se vio muy reducido. Consecuencia de esta eclosión de la imprenta es que en los dos primeros siglos de existencia de la misma, durante los cuales no hubo restricción de copia, se producen

la mayoría de textos literarios universalmente reconocidos y desarrollan su obra algunos de los mayores genios de la historia de la literatura, entre ellos Shakespeare en la cultura anglosajona, Molière en el mundo francófono y Miguel de Cervantes en la literatura hispana.

Sin embargo, hasta que surgen los movimientos revolucionarios no dan los primeros intentos de controlar la información mediante la restricción de copia, justificados con la concesión de ayudas a los editores. Con el acceso a más y más libros impresos y los deseos de libertad del pueblo, el control del flujo de información en las imprentas resultó ser un eficaz método de censura, al menos mientras el precio de las imprentas fue lo suficientemente caro como para provocar su escasez.

En la actualidad, la facilidad para copiar, transmitir y acceder a la información es enorme. Y aunque las ansias de control de la información por parte de los poderes económico y político siguen siendo las mismas y éstos continúan intentando implantar el mismo ecosistema de información escasa que ha regido el mundo hasta ahora, la información fluye cada vez más. No obstante, el control de la información sigue siendo una aspiración evidente de la

mayoría de los Estados. Por ejemplo, en Estados Unidos censuran las imágenes de los cadáveres de los soldados fallecidos en la aún vigente guerra de Irak; la cobertura informativa del regreso de los soldados muertos en combate está prohibida desde 1991. Para Estados Unidos, sus soldados muertos no existen y no se los puede mostrar en público.[34]

Como parte de evitar este tránsito de información fuera del control de las élites políticas y económicas, la restricción de copia ha superado claramente todo lo concebible y ha dejado de ser una modesta ayuda a un editor para convertirse en una esquilma continua de los ciudadanos y sus libertades de uso respecto de los productos que compran.

Pero un sistema que se mantiene gracias a la escasez de información en un entorno que es absolutamente propenso a la generación de abundancia necesita la participación de restricciones digitales para funcionar. Parte indispensable de la generación de escasez, la restricción de copia se apoya en medidas técnicas y, de una forma aún más decisiva, se apoya en medidas legales, como las representadas por la Ley de Propiedad Intelectual en España o la DMCA (Digital Millenium Copyright Act) en Estados

Unidos. Estas leyes imponen limitaciones en el uso de la información y pretenden reducir el número de vías por el que una porción finita de información (definiendo de forma genérica todo tipo de contenidos) se puede retransmitir, modificar y criticar.

Estas medidas de control han sido un signo definitorio habitual de los estados totalitarios, pero medidas de control como éstas se utilizan con cierta regularidad para bloquear el acceso a determinada información también en países democráticos. Es el caso de determinados países, que no permiten que se muestren imágenes de sus soldados fallecidos en combate para seguir manteniendo el apoyo popular a acciones indeseadas, como podría ser una guerra; sin duda todos recordamos la negativa del gobierno estadounidense a mostrar en televisión los ataúdes de sus soldados muertos en la guerra de Irak.

4.1.2. De las personas

La globalización, tal como está enfocada actualmente, es un sistema en el que todo puede circular libremente excepto las personas. El dinero por supuesto, puede circular de unos países a otros, también las

mercancías y las empresas que las producen (las famosas deslocalizaciones), pero no las personas. Para poder cruzar las fronteras, las personas necesitan pasaportes y visados que a menudo tardan meses en ser concedidos.

A veces el enemigo del Estado, cuando se trata de regímenes cuyo gobierno no es justo y es incapaz de mantener contenta a la población, es interno. Las mayores dictaduras del siglo XX eran sociedades bajo vigilancia, y más allá de ese carácter dictatorial, dicha vigilancia parece extenderse por un Occidente en el que se está desmantelando el estado del bienestar sin que la sociedad sea consciente de las consecuencias a medio y largo plazo de las políticas económicas actuales, con el descontento social que originará en el futuro más cercano.

En esas condiciones, el Estado necesita controlar a las personas. Amparados en la política del miedo, los políticos promueven sistemas de vigilancia masivos, diseñados para registrar los movimientos y las actividades de todas y cada una de las personas, en lugar de concentrarse en aquellas a las que considera sospechosas. Con esta doctrina nos convierten a todos en sospechosos, aunque jamás hayamos roto un plato. Esto podría dar lugar a

detenciones preventivas e injustas, más propias de una dictadura que de una democracia, como la que sufrió David Solnit al viajar de Estados Unidos a Canadá en fechas previas a una cumbre en la que se iba a debatir sobre la ampliación del Tratado de Libre Comercio de América del Norte (ALCA, Área de Libre Comercio de las Américas)[35] o las que sufrieron muchos dirigentes socialistas en España en vísperas del primero de mayo en la década de los setenta, cuando, tras el franquismo, emergía una débil democracia.

Es importante no olvidar que a los Estados les importa bastante poco lo que suceda a nivel ciudadano en otros países, y no suelen inmiscuirse salvo cuando afecta a sus intereses. Los gobiernos hacen sus negocios si les interesa, pero no responden en nombre de libertades ajenas. Se reúnen con empresarios y firman contratos cuando les conviene (Estados Unidos bloquea a Cuba pero hace negocios con China y las monarquías del Golfo; España hace negocios con Guinea y con China, y también vende armas a Israel y países donde se violan los derechos humanos).

El control de las personas es principalmente un control dentro de las fronteras, y se depura y fortalece cuando los Estados comparten información sobre sus

ciudadanos a cambio de obtener información de otros ciudadanos. Lo más relevante del control interno por parte de los Estados es que si un Estado te controla en exceso, ningún otro estado del mundo va a mover un dedo para ayudarte. Así que sólo nosotros, los ciudadanos, podemos poner cortapisas al poder para mantenerlo en un nivel que nos ofrezca seguridad sin violar nuestros derechos.

4.1.3. Hacia un mundo sin dinero en efectivo

Mucho tiempo atrás, cuando alguien quería obtener información masiva sobre otra persona revisaba inspeccionaba los desperdicios que había arrojado a la basura. Éste era sin duda uno de los métodos que más información permitía recoger sobre las personas. Con esta técnica podíamos saber si nuestro espiado se alimentaba de comida basura, si compraba primeras marcas, si la noche anterior había comido huevos o si había estado haciendo limpieza de papeles en su estudio.

La aparición de la tarjeta de crédito hace algo más de cuarenta años se anunció como una auténtica revolución. De repente podíamos viajar o ir de compras llevando en el monedero la cantidad justa de dinero, y todo nos parecía

algo más seguro. Y es así: estoy seguro que todos las usamos y procuramos llevar poco dinero encima, pero abusar de ellas tampoco es la mejor opción. La construcción de perfiles comerciales en función de lo que consumimos y lo que hacemos es la responsable de la revolución de las técnicas de venta de los últimos años y el empleo de sistemas de pago trazables permite que la información de compras asociada a nuestra persona aumente progresivamente.

No podemos obviar que los gastos que se pagan con una tarjeta de crédito son perfectamente trazables. Esto significa que se puede ir desde el lector de tarjetas de crédito del establecimiento de turno directamente hasta la puerta de la casa de uno, y conocer por el camino todos los detalles de la transacción (quién, qué, cómo, cuándo, cuánto, dónde). El mismo nivel de trazabilidad nos encontramos si decidimos utilizar tarjeta de fidelidad de un establecimiento cualquiera.

Actualmente sólo hay una forma de pago que nos permite evitar completamente el circuito de la trazabilidad de nuestros gastos: el pago en efectivo. Sólo con el gesto de abrir la billetera y buscar en ella un billete de veinte euros nos aseguramos de que nadie pueda mirar en una base de

datos y saber qué marca de preservativos, gel o aceite de oliva compramos. Sólo si pagamos en efectivo nadie podrá saber qué libro hemos comprado, sea cual sea este libro.

Sin embargo, todos suspiran por saber qué compramos: el supermercado y sus legiones de publicistas para saber más sobre nosotros y así dirigir mejor su publicidad hacia nuestra persona, vendiendo más y mejor; el Estado para mantener su seguridad, que no tiene por qué coincidir con la seguridad de sus ciudadanos. En la democracia actual no es especialmente preocupante, pero en un entorno político más peligroso quizá alguien podría mostrar un inquietante interés por saber si usted lee a Bertolt Brecht, Noam Chomsky, Haro Tecglen, Karl Marx, Primo de Rivera o Pío Moa. Todos ellos son amados y odiados por una parte de nuestros políticos, y el que ahora vivamos en un régimen que respeta nuestros derechos y las libertades de expresión y de información no significa que siempre vaya a ser así.

El mundo sin dinero efectivo sirve tanto para controlar la información como para controlar a las personas. El sistema legal actual persigue establecer un sistema de suscripción a la información, que será enviada vía *streaming*,

la denominada *jukebox*[36] global, y nunca podrá ser almacenada localmente, algo que se quiere conseguir empleando restricciones digitales o DRM. En un mundo sin efectivo, que obligará a pagar de forma trazable cada vez que queramos acceder a información, mantener un registro de quién accede a qué es extremadamente sencillo y se pueden producir abusos con facilidad. Como nunca se sabe en qué mundo vamos a vivir mañana, vale la pena luchar para que el dinero en efectivo siga teniendo su utilidad y su cuota de protagonismo, evitando que sea totalmente reemplazado por los pagos a través de Internet y las tarjetas de crédito.

4.2. RFID

RFID es el acrónimo de *Radio-frequency Identification*, o identificación mediante radiofrecuencias en español. Se utiliza normalmente para definir no sólo el proceso de identificación, sino también los dispositivos usados para llevarla a cabo, los chips RFID. La identificación mediante radiofrecuencias es un pequeño milagro tecnológico y se están planeando un conjunto de aplicaciones beneficiosas, pero sin un control adecuado puede generar una serie de problemas de privacidad.

Estos dispositivos de identificación mediante radiofrecuencias funcionan sin necesidad de contacto entre la tarjeta y el lector: no se utilizan del mismo modo que utilizamos una tarjeta de crédito, acercando la tarjeta RFID al lector, ya que ni siquiera es necesario sacarla de la cartera o el bolso.

La RFID tiene unos límites que no han sido debidamente evaluados y sobre los que los grupos encargados de su comercialización levantan constantemente una cortina de humo que sirva de parapeto para su negocio. Esta tecnología representa actualmente una gran amenaza para nuestra privacidad. Los chips RFID son tan pequeños (algunos tienen un área de 64 μm^2, y su tamaño se reduce cada vez más), que son susceptibles de ser incluidos, literalmente, en todas partes: desde piezas y recambios de vehículos hasta billetes de euro o simple papel de oficina, pasando por maquinillas de afeitar, pasta de dientes o ropa interior.[37]

Aunque para muchas personas es una gran desconocida, la precursora de esta tecnología tiene más de medio siglo de vida y la primera patente de RFID data de 1973, cuando la presentó Charles Walton.[38] La tecnología de

identificación por radiofrecuencias está ya ampliamente extendida en nuestro entorno y la podemos encontrar actualmente en entornos y aplicaciones tan dispares como los abonos de transporte de las principales capitales europeas (París, Londres, Barcelona o Madrid entre ellas),[39] los transpondedores que se utilizan en muchos edificios de oficinas y, lo que es más preocupante, en los pasaportes de numerosos Estados, incluido el pasaporte que desde el 28 de agosto de 2006 emite el Estado español;[40] y hay algo especialmente inquietante: los chips están ahí, pero nadie se ha enterado de que su pasaporte lleva uno de ellos.

4.2.1. El chip RFID

Siempre que se habla de RFID se da por supuesta la existencia de un microchip que gestiona la información y que es el que, en última instancia, realiza la identificación. Un chip RFID o etiqueta RFID es un dispositivo electrónico, altamente miniaturizable, que se puede comunicar con otros dispositivos mediante la emisión y recepción de radiofrecuencias, y que puede permanecer funcional durante una cantidad indefinida de tiempo, teóricamente infinito en el caso de los chips RFID pasivos. En estos chips se introduce una determinada información, que el chip se

encarga de emitir en determinadas circunstancias. De este modo almacenamos una información que podrá ser leída posteriormente de forma inalámbrica y remota, hasta una distancia que varía según el tipo de chip RFID de que se trate. Esta distancia puede oscilar entre unos pocos centímetros y varios centenares de metros.

Lo que convierte a la tecnología RFID en una amenaza para la privacidad es el hecho de que cada chip RFID está dotado de un identificador único. ¿Qué significa que tiene un identificador único? Para esto, y sólo para esto, voy a utilizar la comparación con un código de barras, pues en todo lo demás son muy diferentes. En los sistemas de etiquetado actuales, cada tipo de producto tiene un código asociado que sirve para clasificarlo y para que al pasarlo por la caja del supermercado la máquina sepa que estamos comprando leche y no galletas, de manera que nos indique (y nos cobre) el precio de la leche y no el de las galletas. Esto se deba a que el código de barras es un código genérico que técnicamente se conoce como Código Electrónico de Producto o EPC (Electronic Product Code). El que los chips RFID tengan un identificador único significa que cada paquete de galletas tiene su propio código, distinto al de

cualquier otro paquete de galletas. Esto hace posible el seguimiento a través del espacio y del tiempo de diversos productos. Y el seguimiento se realiza para un producto en concreto: no se monitoriza un paquete de maquinillas de afeitar, sino que se monitoriza *tu* paquete de maquinillas de afeitar, asociado a tu persona, ya que posiblemente pagaste con tarjeta. Este código único de producto se conoce como Código Universal de Producto o UPC (Universal Product Code).

Cómo funciona un chip RFID

Un chip de radiofrecuencias permanece en letargo mientras no reciba una señal (emisión de radiofrecuencias) que actúe como disparador. Una vez recibe esta señal, se desencadena la activación del chip, que utiliza la energía recibida para leer la información que contiene y reemitirla. El funcionamiento del chip finaliza con el envío de una nueva señal de retorno, también de radiofrecuencias, que eventualmente será recogida por un lector de radiofrecuencias.

Los chips RFID se pueden clasificar en activos y pasivos atendiendo a su diseño, según incluyan, o no, una

batería que permita amplificar la señal que emitirán. A los que no incluyen esta batería se los llama pasivos y su alcance oscilas entre varios centímetros y varios metros; a los que incluyen batería se los llama activos y su alcance es muy superior, hasta varios cientos de metros.

En vistas de ello, se podría pensar que los chips activos son más peligrosos para la privacidad, pero no es así; es más, la realidad es exactamente la contraria. Un chip activo tiene un tiempo de vida limitado por su batería: tan pronto como ésta se agota, el chip se apaga hasta que reemplacemos la batería. Por contra, un chip pasivo no requiere batería, y la energía necesaria para su funcionamiento la obtiene de la señal de radiofrecuencias que lo activa. Como no necesita batería, el tiempo de vida de un chip RFID pasivo no está limitado, y volverá a enviar la información que contiene indefinidamente, cada vez que reciba una señal de disparo. Esto podrá suceder durante un tiempo indefinido, hasta que el chip se deteriore.

Cada vez que se dispara, un chip RFID produce una misma señal de salida. Esta señal porta la información contenida en el mismo y su identificador único. Por ello el apelativo de «chips inteligentes» con que los fabricantes se

refieren a estos dispositivos, y que aparece hasta la saciedad en todos los panfletos, no puede ser más desacertado. ¿Qué clase de inteligencia se limita a repetir una y otra vez algo que ha memorizado, sin cambiar un ápice la respuesta?

4.2.2. La mitología alrededor de los chips RFID

Los chips RFID están rodeados de un aura publicitaria enorme de la que es responsable la industria que los produce. Esta industria es tan consciente de los problemas que plantea dicha tecnología que en una de sus últimas cumbres anuales (RFID Industry Summits) ha llegado a admitir que «la tecnología RFID ha alcanzado una difusión tal, que la industria pronto comenzará a enfrentarse a problemas legales».[41] Si un portavoz de la industria que nos lo intenta vender admite esto, ¿hasta qué punto estará al margen de la legalidad el mencionado invento?

La mitología de la RFID incluye toda clase de portentos, y la mayoría de ellos oscilan entre la falsedad y la total irrelevancia: la reducción de tiempo en las colas, la facilidad de acceso a nuestros espacios, las mejoras en la capacidad de clasificación.

Primer mito: la RFID eliminará las colas en los supermercados y en los tornos de las estaciones. Supuestamente, no es necesario sacar del carro y poner delante del lector láser de la caja una compra en la que todos los productos incluyan una etiqueta RFID. La compra se revisaría simplemente pasando nuestro carro de la compra por un arco de radiofrecuencias y el importe total se cargaría a nuestra tarjeta de crédito. De esta manera no hay que pararse en la caja y no estorbamos a la persona que viene detrás. Se trata de una falacia risible. Este acto, que todo el mundo concibe como una ventaja (ahorro de tiempo) y que afecta directamente a una de las actividades más odiadas por el ciudadano medio (ir al supermercado después del trabajo o en su único día libre de la semana), es irrealizable a no ser que pretendamos cambiar absolutamente el mundo en que vivimos, renunciando a muchos de nuestros derechos. Veamos los fallos uno a uno. En primer lugar, es necesario que cada producto tenga un chip RFID. Por la diferencia de precio existente entre ellos, éstos serán siempre pasivos. Pero además es necesario que mi tarjeta de crédito tenga a su vez un chip RFID que pueda ser leído por la caja automática. El importe se carga directamente en mi tarjeta, sin que yo firme un recibo ni

teclee mi número personal. Además, no se emite ningún recibo o factura que actúe como garantía de compra. A menos que pretendamos modificar de raíz el modo en que desarrollamos nuestra vida diaria, todos estos inconvenientes suponen un problema que arruina todo ahorro de tiempo. Pues al final todos ellos se solucionan con la presencia de una persona en la caja que realice las operaciones. Y para ahorrar esta pequeña cantidad de tiempo, estimada como promedio en alrededor de 20-30 segundos por cliente, necesitamos aceptar que nuestra tarjeta de crédito tenga un chip RFID, que sea leída automáticamente, que se nos cargue un importe de compra automáticamente (algún producto podría estar mal etiquetado en su estantería y no lo sabríamos nunca) y, para colmo, que no haga falta nuestra firma para cargar la compra en nuestra tarjeta. Por último, al haber pagado con tarjeta de crédito, todos esos chips RFID de nuestros productos son vinculados a nuestra persona y, al no haber recibido ningún recibo de compra, la única garantía posible recaería precisamente en el chip RFID, que no podríamos desactivar, so pena de quedarnos sin garantía. Nos convertimos en un abrir y cerrar de ojos en el cliente soñado del supermercado: el que compra rápido y paga sin

rechistar.

Primer mito, parte segunda: la RFID reducirá la cola para entrar y salir de autobuses, metros y trenes. Según este segundo mito, el simple paso por la entrada o salida de cualquier transporte público servirá para identificarnos, sin necesidad de pasar por tornos y ahorrándonos el tiempo necesario para ello. Dejando de lado que las colas para entrar y salir del metro a través de los tornos rara vez te hacen perder más de 5 segundos (a veces ni eso), de nuevo el principal problema está en todas las imposiciones que hay que aceptar para poder ahorrar esos segundos: necesito portar una tarjeta RFID. Esta tarjeta RFID no tiene por qué estar necesariamente asociada a nuestra persona, como sucede en Málaga con el abono multiviajes, pero en la mayoría de transportes públicos los abonos mensuales, así como las tarifas de descuento, están reservados a las tarjetas RFID nominales. Así sucede en Londres con la Oyster Card, en Lisboa con la Tarjeta 7 Colinas o en París con Navigo, por citar tres ejemplos.[42] De esta forma, cada vez que uno se sube al autobús, se está identificando unívocamente. Incluso en el caso de que la tarjeta RFID de dicha persona no contenga información personal, las asociaciones en las bases de datos

la acabarán vinculando con ella. Por ejemplo, si cada vez que se lee el chip de una tarjeta de transporte se lee también el chip RFID del pasaporte de una persona, o de cualquiera de sus objetos personales (por ejemplo, los zapatos que posiblemente pagó con su tarjeta de crédito y que pueden ser vinculados a esa persona).

Segundo mito: control de acceso más seguro. Los chips RFID posibilitan la identificación unívoca de los objetos y de las personas. Esto permite imponer férreos controles de acceso adaptados a cada uno. Donde antes había una llave física que podías utilizar sin límites ahora hay una llave electrónica asociada a tu persona y, quizá, a un número PIN que hay que teclear. De esta forma se consigue que el acceso a los espacios privados esté muy limitado, por ejemplo en el ámbito empresarial, restringiendo los departamentos de la oficina a los que se puede entrar y a los que no, así como sus horarios y fechas límites. Se supone que estos accesos son más seguros, pero habría que ver de parte de quién está esa llamada a la seguridad. Todo parece indicar que la persona que entra en un edificio con este tipo de llaves está sometida a una vigilancia constante. Se pueden vigilar las entradas y salidas del despacho, su

duración; las entradas a la cafetería, el tiempo de permanencia en la cafetería y su frecuencia; la compañía, pues todo el mundo lleva un chip; la frecuencia y duración de las visitas al servicio. Está claro que estas tarjetas RFID ofrecen seguridad de acceso, pero no está claro a quién ofrecen facilidad de acceso. Por otra parte, nada impide que una persona abra la puerta con su identificación y, una vez abierta, entre más de una persona. Esto se conoce con el término inglés *tailgating* y es otro motivo para pensar que la utilización de RFID no confiere seguridad a las instalaciones.

Tercer mito: la RFID mejora la capacidad de clasificación de los objetos. Esto es, posiblemente, cierto. Se pueden incluir chips RFID en todos los objetos para poder localizarlos mejor: las llaves de casa, las del coche, etc. Esta facilidad para localizar e inventariar es la principal justificación que la industria ha ofrecido a la sociedad para extender sus microchips por todas partes. Sin embargo, esta capacidad tiene un caballo de Troya incluido: para que todo sea perfectamente localizable, desde mis zapatos hasta las llaves de mi coche, necesita tener un chip RFID incrustado. Ello permite, en teoría, que se pueda trazar perfectamente la trayectoria de nuestras pertenencias, así como el tiempo que

se tarda en realizar un determinado trayecto. Podría darse el caso de que nuestra nevera tuviera un lector RFID incorporado, de forma que cada vez que sacáramos un envase de leche lo anotara y cuando sacáramos el último encargara automáticamente más a nuestro supermercado. Esta posibilidad es especialmente grave porque permite a los supermercados conocer cómo usamos las cosas que compramos, ayudándolos a optimizar los mensajes de publicidad que nos envían. Para quienes piensen que esto aún está muy lejos, esta nevera ya existe y se puede encontrar cada vez en más hoteles, sobre todo en hoteles de lujo, ya que -no se engañen, nadie regala nada- de quien más interesa conocer los hábitos, para poder venderle más y mejor, es precisamente de la gente que más dinero puede gastar. Está claro que la RFID ofrece una ventaja gracias a su capacidad para la identificación unívoca de productos y su potencial de localización exacto. Lo que no parece tan claro es que esa ventaja lo sea para mí, simple mortal, sino más bien para el mayorista, que puede seguir estudiando el uso de sus productos incluso mucho tiempo después de haberlos vendidos. Y sin pagarnos nada por toda la información de uso que le regalamos.

Éstos son los tres pilares sobre los que monta su estrategia de venta e implantación la industria del RFID: no parece un soporte muy sólido.

4.2.3. El problema de los chips RFID

El problema de privacidad relacionado con los chips RFID estriba en que no podemos controlar quién lee los chips, cuándo los lee ni hasta cuándo podrá leerlos. Esta situación se agrava en el caso de los chips pasivos, en letargo permanente a la espera de una señal que los dispare. Esa definición del problema sólo menciona una parte del mismo: el verdadero problema es que el identificador único de estos chips se puede vincular fácilmente a nuestra persona, lo que constituye en sí mismo un problema para nuestra privacidad.

4.2.4. Control gracias a RFID

Las capacidades de control que la tecnología RFID ofrece son casi tan ilimitadas como pequeño es su tamaño e inalámbrica su conexión. Los chips tienen un tamaño mínimo, almacenan cada vez más información y no se necesitan cables para transmitirla, por lo que controlar quién accede a la información almacenada de esta manera es

harto difícil. Esto hace posible no sólo que se utilicen con fines publicitarios, sino que permiten ejercer un gran control sobre las personas gracias al conocimiento que podemos extraer de su actividad cotidiana a través de estos chips.

¡Cuidado, te siguen!

La monitorización de personas en tiempo real es sin duda la aplicación más llamativa de la tecnología RFID. Saber cuándo se mueven y cuándo se detienen, dónde entran, cuánto tiempo permanecen allí y si portan algo que antes no portaban. Las aplicaciones de estas tecnologías a las técnicas de venta son el sueño de todo vendedor; las aplicaciones al control de personas son la pesadilla de todo disidente en tiempos difíciles.

Este seguimiento podría parecer fantasioso e improbable, pero no lo es. Y aunque la mayoría de nosotros no habríamos pensado nunca en utilizar estos chips para el seguimiento de personas, está claro que hay alguien que sí lo pensó, y lo patentó. Si hay una patente que ha levantado ampollas en aquellos que temen por el modo en que su libertad y su privacidad van a ser tratadas en un futuro, ésa

es la patente de *IBM*, que describe un sistema para monitorizar de personas espacios cerrados.[43] La patente fue solicitada en 2001 y concedida en 2002 en Estados Unidos, y constituye la principal demostración de lo que la industria ve tras esta tecnología: capacidad de monitorizar lo que las personas hacen siempre y en todo momento, capacidad para estudiar a las personas. Control. No será necesario que una persona nos siga todo el día para espiarnos, los chips que llevemos encima se encargarán de todo.

Rediseñando la red con ayuda de la RFID

La red, tal y como está diseñada actualmente, permite la entrada y salida del sistema con mucha facilidad. Todo lo que tiene que hacer quien desee conectarse es ceñirse a unos protocolos, los protocolos que gobiernan la red: TCP/IP, HTTP, FTP, etc. ¿Qué sucedería si la red, tal y como la conocemos hoy, fuera modificada para imponer un control mediante RFID, previo a permitir la conexión de un nuevo dispositivo a la misma?

Rediseñar la web requiere una capacidad de computación enorme: los protocolos TCP/IP son prácticamente ubicuos. Pero, y ¿si para rediseñar la web en

lugar de cambiar el protocolo que la gobierna por otro que actúe de control lo que hacemos es imponer un control previo a la conexión? Evidentemente los sistemas actuales, que no tienen empotrado el control, es posible que funcionaran igualmente durante un tiempo. Más adelante, la incorporación del control podría ser obligatoria: estos viejos dispositivos se irían rompiendo y serían reemplazados por nuevos elementos sometidos a este control. Con el tiempo serían una especie en extinción y no habría necesidad de reprogramar la red. No habría que rediseñar nada, sólo añadir una nueva capa de cebolla que lo envolvería todo: la capa de cebolla de la RFID.

Cómo funcionaría

Imaginen un punto de acceso wi-fi que sólo permite acceder a la red a aquellos dispositivos que se identifican con una etiqueta RFID permitida; imaginen, si aún no lo han hecho, que todos los puntos de acceso wi-fi pidieran una etiqueta RFID permitida para acceder a la red. A partir de la aceptación de la etiqueta, la red funcionaría como funcionan todas las redes que conocemos, pero con la diferencia de que se invadiría tu privacidad, ya que puedes cambiar de alias en la red, borrar tus *cookies*, tu *cache* y cambiar la MAC

de tu tarjeta de red, pero no es probable que vayas a cambiar la etiqueta RFID que viene incrustada en el microprocesador de tu portátil o de tu móvil. Ni que decir tiene que es improbable parece difícil que cada vez que te conectes a la red uses una computadora distinta. Y también parece poco probable que esas computadoras no puedan ser vinculadas directamente con tu persona (¿cuántas personas conoces que compren sus ordenadores en metálico sin identificarse?). Ese punto de acceso ya no obedece a un protocolo: para acceder al protocolo hay que pasar un control; dime quién eres y dónde estás, y yo te diré si tienes derecho a atravesar la puerta. Apple solicitó una patente para gestionar conexiones de red entre dispositivos utilizando identificación por radiofrecuencias.[44]

De esta forma desaparece la posibilidad de conectarse a una red libremente, como hacemos actualmente. Disidentes políticos o activistas, que podrían sufrir represalias por sus opiniones, serían automáticamente detectados gracias a este identificador y localizados tan sólo con conectar sus máquinas. El sólo hecho de conectarse a la red los delataría; más aún: si el identificador RFID de su máquina es vetado en la red, les sería imposible conectarse.

Además, el anonimato, ya seriamente dañado en la red actual, se vería muy debilitado. Si esta persona decide hacer público un escándalo de corrupción política o empresarial, podrían identificarlo aún más fácilmente de lo que se puede en la actualidad y esa persona podría perder su trabajo o enfrentarse a una causa penal por hacer algo tan loable como denunciar un comportamiento ilegal; en regímenes no democráticos esto supone un problema real que podría conllevar penas de cárcel o incluso peores. Por eso este tipo de red no es deseable. El problema de la ciberdisidencia fue analizado por Reporteros sin Fronteras, que en 2007 publicó un *Manual para bloggers y ciberdisidentes*.[45]

4.2.5. Chips RFID subcutáneos

El hecho de que cada chip tenga un identificador único que se puede leer de forma inalámbrica posibilita la identificación de personas utilizando chips RFID implantados bajo la piel, lo mismo que posibilita la identificación de animales domésticos, como en el caso de los perros, que en España tienen que llevar implantado uno de estos chips. Estos chips han sido desarrollados por *VeriChip*,[46] empresa que, además, tiene la patente de explotación exclusiva de estos dispositivos.

El primero de estos implantes en humanos de que se tiene constancia le fue realizado en 1998 a Kevin Warwick, profesor de cibernética en la Universidad de Reading (Reino Unido).[47] También es muy conocido el caso de Amal Graafstra, quien en 2005 se implantó dos de estos chips.[48] Aunque estos chips fueron implantados en las manos, se estima que la zona más sensible para su implantación es bajo los omoplatos, ya que es ahí donde, una vez recuperados los tejidos en torno al chip, resultaría más difícil su extracción. Estos chips para implante subcutáneo son más grandes que un chip RFID convencional, aunque mantienen unas dimensiones relativamente pequeñas. Están encapsulados bajo una forma cilíndrica con una longitud de aproximadamente un centímetro y un diámetro de tres o cuatro milímetros. Desde luego, son bastante más grandes que *un grano de arroz*, eslogan utilizado en la campaña publicitaria, aunque lo suficientemente pequeños para ser implantados sin que sean perceptibles en ausencia de un detector de radiofrecuencias.

Ya se han diseñado métodos para la vigilancia de personas usando estos chips y sólo falta su extensión a numerosos ámbitos de nuestra vida cotidiana, algo que

sucederá si no logramos antes una reforma legal que regule su uso. Los primeros pasos para lograr su aceptación social se han dado usando la herramienta del sentimiento blando: utilizando estos chips en centros con enfermos de Alzheimer y otros pacientes de «alto riesgo».[49] La promesa es que ofrecen a dichos enfermos una atención continua cuando sucede literalmente todo lo contrario: se sustituye la atención del personal sanitario que vigila a los pacientes por chips de radiofrecuencias que permiten saber la localización de los enfermos sin que nadie vigile a esas personas. Se ignora el hecho de que los enfermos y las personas mayores necesitan un trato humano y digno que no puede ofrecer un sistema como éste. También se han empleado para el control de reos, aunque en este caso se prefiere usar un microchip en forma de brazalete electrónico, y no el que se implanta bajo la piel.[50]

Además de las aplicaciones para controlar a enfermos y presos, se han utilizado como objeto de moda en algunos bares alrededor del mundo. En éstos, los clientes se instalan un chip bajo la piel que asocian a su persona y a su tarjeta de crédito, de forma que las consumiciones se abonan automáticamente. A veces se exige como requisito y

sólo pueden tener acceso al local las personas que llevan un determinado identificador RFID.[51]

Sin embargo, el problema subyacente en estos chips no es que un determinado local exija su implante para acceder. Siempre ha existido el derecho de admisión y ésta es tan sólo una forma más esnob de implementar ese control. El problema es que, como todo chip RFID, el *VeriChip* emitirá una misma señal continuamente que permitirá identificar a una persona por proximidad, aunque ésta se encuentre fuera de nuestro campo de visión al otro lado de una pared o una puerta, aunque ésta jamás llegue a saber que la hemos identificado ni pueda evitar la emisión de su chip. Y ése es precisamente el problema, que permitirá identificar a una persona de forma continua sin otorgar a la misma la capacidad de decidir cuándo quiere permanecer identificable y cuándo no.

Éste ha sido el principal factor que ha hecho que en determinados lugares, como California, se prohíba la implantación de uno de estos chips como condición necesaria para optar a un puesto de trabajo,[52] lo que viene a eliminar una actividad que comenzaba a extenderse: exigir estos implantes para optar a determinados trabajos de alta

responsabilidad (vigilancia de cajas fuertes y custodia de determinadas instalaciones). Estas medidas representan todo un hito pero, como comentaba George Ou, «Ahora me siento respaldado en mi estado pero, ¿por qué esta prohibición no es de ámbito federal?».[53] Y también por el matiz mencionado en el comentario publicado como respuesta a esta afirmación: «No es sólo cuestión de tener un problema con los implantes en sí mismos; aunque no tuviéramos problemas con estos implantes, tendríamos que tenerlos con todo aquel que pretenda forzar su implantación».[54]

Pero no se trata sólo de eso, o de que estudios médicos hayan vinculado el implante de estos chips al crecimiento de tumores:[55] si hay algo peor que estar identificado todo el tiempo, se desee o no, es que puedan existir errores en esa identificación, de forma que se pueda culpar a alguien de algo que haga otra persona si el sistema cree que es culpable.

Existe un agravante de todo lo anterior: el que el sistema de identificación sea tratado por las instancias públicas como infalible. Este tratamiento de infalibilidad hace que toda reclamación por un error en la identificación

pueda considerarse un intento de burlar la ley y, eventualmente, sea desestimada. Los chips de *VeriChip* para implante subcutáneo, como cualquier otro chip RFID, han sido clonados.[56] Esto significa que la información contenida en los mismos ha sido copiada y luego introducida en un nuevo chip que emitirá exactamente la misma información que el original. La clonación de estos chips contradice la afirmación que los vendedores de esta tecnología han utilizado para promover la RFID y su utilización en sistemas de identificación personal para pagos y otras tareas sensibles. Si estos chips pueden ser clonados, su uso para identificación no es fiable y se debe evitar de forma tajante.

4.2.6. Documentos de identidad y RFID

La inclusión de las etiquetas RFID es una de las mayores apuestas de control realizadas por los Estados. Muchos países occidentales emiten pasaportes RFID desde 2006, cuando algunos países como Estados comenzaron a exigirlos para acceder al país. Todos los pasaportes emitidos en España desde agosto de 2006 incluyen un chip RFID.

La introducción de la RFID en documentos oficiales es mucho más alarmante que cualquier otro chip RFID que

pueda encontrarse y se está extendiendo a toda prisa porque los gobiernos, sabedores del rechazo que genera, quieren asegurarse de que el debate no llegue al gran público hasta que la red RFID esté ya bien asentada. Al fin y al cabo, luchar por eliminar una infraestructura es mucho más difícil que detener su extensión en primer término. La oposición a la inclusión de este tipo de identificadores en documentos oficiales se relaciona con los problemas de privacidad pero, por encima de lo que es la simple defensa de nuestra intimidad para evitar molestias publicitarias, sobre todo se relaciona con la defensa de las libertades civiles básicas en nuestro futuro más cercano.

¿Por qué incluir en nuestros documentos un chip RFID? Este chip no sirve para nada que no sirvan otros mecanismos previstos en nuestro derecho y, además, añaden un componente de inseguridad gratuita: estos chips los puede leer cualquiera y los puede clonar todo aquel que posea los conocimientos necesarios.

Los problemas de privacidad afloran rápidamente. Estos chips contienen todo tipo de información personal que podría leer cualquier persona. Antes de seguir adelante háganse a sí mismos esta pregunta: ¿dan su número de

teléfono privado a cualquier persona que se cruzan en la calle? No, evidentemente no le damos nuestros datos a cualquiera, sino a aquellos que queremos que los tengan. Con la inclusión de estos chips en los documentos de identidad (como pasaportes o tarjetas de identidad estatales) cualquiera con un lector de RFID podrá saber todo sobre nosotros (nombre, apellidos, dirección, fecha de nacimiento, etc.).

Lo siguiente es considerar cuánto cuestan estos dispositivos. Quizá son caros, lo que significaría que no todo el mundo puede acceder a ellos. Pero ahí están los datos: el fabricante noruego de teléfonos móviles Nokia ya pensó hace un par de años incluir un lector de RFID de serie en sus teléfonos.[57] No parece que vaya a ser un dispositivo exclusivo, de difícil acceso e implantado en un futuro lejano. Imagine por un momento que, en lugar de un compañero de trabajo pesado pero inofensivo (lo cual ya sería bastante serio), tiene acceso a los datos de sus documentos RFID una persona mucho más peligrosa. No podrá evitar que esa persona peligrosa tenga acceso a sus datos personales. n pasaporte de este tipo incluye datos identificativos e información biométrica del dueño del pasaporte. Y la

etiqueta RFID se limita a transmitir todo el tiempo dicha información, a todas las personas que la activen.

Otro tipo de problemas derivado del uso de estos chips en documentos de identidad es el robo de la misma. Este chip puede ser clonado y lo ha sido en repetidas ocasiones.[58] Con esta clonación, cualquiera puede ir por ahí con un chip que le permitirá identificarse en mi nombre y que engañará a las máquinas haciéndolas creer que en realidad soy yo el que transita por una calle que jamás he pisado, el que roba en una tienda que jamás he visitado, el que hace cientos de cosas que jamás he hecho. La clonación de pasaportes RFID abre un camino tecnológicamente viable para la suplantación de identidad, y el uso que se pueda hacer de esta suplantación cometiendo algún delito mientras las máquinas piensan que es usted efectivamente el que está allí, es motivo suficiente para que estos chips cargados de información personal sean eliminados de inmediato de los documentos oficiales.

4.3. Videovigilancia

Es posible que no todos los experimentos sociales que se llevan a cabo en las cárceles sean represivos, pero la

gran mayoría sí lo son. Esta lógica obedece al principio básico de dominación: si una técnica represiva resulta exitosa en una población mayoritariamente conflictiva como puede suponerse que es el conjunto de reclusos de una prisión, sin duda esta técnica también resultará exitosa en la difícil tarea de doblegar la voluntad de una población más pasiva, que pese a ser mucho más numerosa será también más mansa y menos conflictiva que la población reclusa.

La videovigilancia forma parte de las tecnologías desarrolladas para el control de reclusos hace varias décadas -del mismo modo que ahora se proponen implantes RFID para los reclusos,[59] algo que debería ponernos en alerta- y recientemente, debido al abaratamiento de la tecnología, se ha extendido por nuestras calles para colonizar nuestras ciudades. Se está comenzando a aplicar a personas libres, inocentes mientras no se demuestre lo contrario, técnicas de control y coacción.

Videocámaras que, además de registrar vídeo, registran sonido y cuyo software les permite diferenciar conversaciones.[60] Videocámaras que te amonestan si muestras un comportamiento poco cívico, como tirar un papel al suelo, mientras registran y almacenan todas tus

conversaciones. Y dicen que no pasa nada, que a nadie le interesa si usted se opone a algún régimen tiránico en Asia[61] o si se opuso usted a Bush en público aquel 15 de febrero.[62] Nadie le preguntará si usted votó izquierda o derecha, si es rojo o azul, monárquico, republicano, católico, protestante, jacobino. Puede dormir tranquilo porque su seguridad e intimidad están a salvo. Eso es lo que nos dicen, pero entonces, ¿para qué sirve todo esto si no es precisamente para conocer los pasos de todos y cada uno de nosotros y utilizar esa información llegado el caso?

Es posible que haga disminuir la delincuencia en la vía pública, aunque más bien lo desplazará hacia otros lugares donde no haya tanta vigilancia, como pueden ser los hogares. Esto se ha observado ya en Yeovil (Reino Unido) como consecuencia de la prueba de un sistema biométrico que obligaba a todos los que entraran en un pub a registrar sus huellas dactilares a la entrada.[63] Nos dicen que esto tiene ventajas, y quizá en parte sea verdad, pero nos ocultan multitud de consecuencias negativas y dañinas. También están ahí, pero nadie habla de ellas.

4.3.1. Ojos mecánicos

La necesidad de vigilar todo lo que sucede, ya sea en entornos cerrados o entornos abiertos, conlleva la obligatoriedad de vigilar a todas y cada una de las personas. En un universo en el que se presupone la culpabilidad y la necesidad de vigilar a todo el mundo, es importante tener en cuenta que el número de personas vigilando sería tan elevado que no se podría pagar a todas ellas y que, aun así, es posible que no se pudieran vigilar todos los rincones.

Aquí es donde la videovigilancia, tal y como la concebimos actualmente, juega un papel principal: en un entorno donde todo el mundo es un potencial culpable, la necesidad de vigilar a toda la población requiere de un número de ojos tan elevado que sería imposible realizar esta función de vigilancia en ausencia de vigilantes automáticos que no perciban sueldo ni descansen. Las videocámaras y sus ojos mecánicos están ahí grabándolo todo para que esté disponible en caso de que no haya ningún policía que pueda cubrir la zona.

Con la tecnología actual podría pensarse que la vigilancia masiva de la población es agrandar el tamaño del pajar en el que queremos buscar la aguja, como opina Pepe

Cervera,[64] pero lo cierto es que, con el aumento de la capacidad de cálculo de las computadoras y la mejora del software de reconocimiento de objetos y rostros en fotografías y grabaciones de vídeo, esta tecnología se presenta como un arma potencial de represión dada la posibilidad de comunicarle al sistema, en tiempo real, dónde estamos y qué estamos haciendo. Estos sistemas no están tan lejos en el tiempo, y la Universidad Carlos III de Madrid ya ha desarrollado un sistema de reconocimiento como este que actualmente se emplea para el reconocimiento de pasajeros en el aeropuerto de Barajas, en Madrid.

4.3.2. Videovigilancia distribuida

Otro concepto de videovigilancia se apoya en la estructura existente actual: una Internet en la que es fácil introducir contenido, el auge de las redes sociales en la red y la accesibilidad a cámaras de fotografía y vídeo digital. El hecho de que cualquiera pueda tomar una foto cuando sucede algo y colgarla automáticamente en la red evita la necesidad de un software inteligente que permita discernir rostros o movimientos bruscos en fotografías y vídeo. Ese software llegará, pero mientras tanto el sistema se apoya en la inteligencia de la población, en nuestra fijación por todo

lo que se sale de lo normal y en la capacidad técnica de grabarlo y transmitirlo a la red.

Implantar este tipo de red de vigilancia es más barato que cubrir con cientos de miles de cámaras nuestras ciudades, pero se necesita la colaboración de la población para fotografiar y delatar a sujetos. Y es aquí donde los mensajes de la política del miedo convierten a los medios de comunicación en una fuente de pánico medido. Es en este contexto donde surgen las alarmistas campañas de pánico introducidas por Reino Unido en sus transportes públicos, que hacen sentir verdadero miedo a la población y animan a delatar y denunciar sin demora a cualquier persona que despierte sospechas.[65] Estos anuncios se utilizaron en Reino Unido a lo largo de 2007, aunque bien podrían haberse utilizado en alguna de las dictaduras comunistas desmanteladas hace décadas. Las viejas tácticas de propaganda soportan bien el paso del tiempo.

En este punto, todo lo que se necesita para obtener la colaboración voluntaria de la población es la existencia de un estado de psicosis ambiental, y cuanto más elevado sea este nivel de psicosis, tanto mejor, como en la campaña del metro de Londres. Ni que decir que el giro orwelliano de

estas medidas es espectacular y las posibilidades de linchamiento social de minorías étnicas o ideológicas es enorme, ya que supone una vía de escape perfecta para todo el racismo inculcado contra la inmigración por un sistema económico, el actual, que basa sus mecanismos de generación de riqueza en mantener a una gran parte de la población mundial excluida de los círculos de comercio y consumo, encerrada en sus países de origen y privada de toda posibilidad de un futuro mejor.

Las reformas legales que llevó a cabo Tony Blair en Reino Unido posibilitan la detención sin pruebas durante decenas de días de cualquier sospechoso de terrorismo. Si una denuncia anónima te convierte en sospechoso, podrás probar las bondades del sistema de seguridad antiterrorista británico. Es muy probable que para cazar a un verdadero terrorista se detenga sin pruebas y se prive de libertad durante meses a cientos de ciudadanos británicos (y extranjeros) inocentes. Es algo que les importa poco, simplemente porque jamás se han parado a pensar que podría pasarles a ellos: todas estas medidas están diseñadas desde la falta de mesura propia del que nunca se ha visto al otro lado de la valla. Una denuncia falsa, y a prisión

incondicional preventiva. Como cabe esperar en una situación legal en que a la policía se le confieren poderes de milicia, la brutalidad de la misma quedó más que demostrada con la muerte de Jean Charles de Menezes, un joven brasileño al que la policía de Londres asesinó en pleno vagón de metro al confundirlo con un terrorista, asesinato que luego trató de encubrir con mentiras.[66] El peligro de leer el periódico en el vagón de metro en tiempos de pánico mediático.

4.4. Biometría

La biometría es una rama de la biología que estudia y mide los datos procedentes de los seres vivos. Sirve para automatizar los procesos de identificación y verificación de un sujeto en función de sus características anatómicas o de su comportamiento.

Habitualmente, llamamos biometría no a la biometría propiamente dicha, sino a la aplicación a la informática de la biometría, o biometría informática. La biometría informática es la aplicación de técnicas biométricas a los procesos de identificación de personas, empleando sistemas electrónicos o informáticos de

seguridad. Las biometría informática utiliza para su funcionamiento técnicas estadísticas y de inteligencia artificial.

Bajo el distintivo común y generalista de biometría se agrupa todo un conjunto de tecnologías de identificación que se caracteriza por utilizar para el proceso de identificación diversos rasgos físicos que permiten diferenciar a una persona del resto.

La biometría, apoyada por la poderosa industria biotecnológica, se abre paso como un método de identificación segura pese a contar con vulnerabilidades que, de producirse un error, tendrían consecuencias aún más severas, ya que la confianza del usuario y la concentración de identificaciones en sólo unos cuantos parámetros harían que una vulnerabilidad en uno de ellos permitiera el acceso no autorizado a un número no estimable de servicios privados, siendo el daño posible incalculable.

Por ello es posible que las ventajas profetizadas por esta industria no justifiquen la implantación de todos estos sistemas de identificación biométrica, que actúan como controles y que nos ofrecen además una falsa sensación de

seguridad cuando en realidad ya se ha demostrado que algunos son vulnerables.

4.4.1. Tipos de biometría

La biometría informática es una rama de la seguridad para las identificaciones que ha avanzado notablemente y se ha desarrollado por muy diversos caminos. Consecuencia de esta evolución es la existencia de un amplio abanico de posibilidades biométricas basadas en distintos parámetros. Estos parámetros se dividen en dos grupos según midan parámetros anatómicos de las personas (biometría estática) o el comportamiento de las personas (biometría dinámica).

La biometría estática comprende y mide la anatomía de las personas. Entre los muchos parámetros biométricos existentes en la actualidad destacaremos las huellas digitales, la geometría de la mano, la disposición de las venas en la palma de la mano, la termografía, el análisis de iris, el análisis de retina y el reconocimiento facial.

La biometría dinámica comprende y mide el comportamiento de las personas. Entre los parámetros que maneja este tipo de biometría destacan el patrón de voz, la

firma manuscrita, la cadencia del tecleo, la cadencia del paso y el análisis gestual.

4.4.2. El proceso de identificación biométrica

En el proceso de identificación biométrica hay que tener en cuenta los elementos del sistema biométrico, las propiedades de los datos utilizados y las fases del proceso de identificación.

El sistema biométrico consta de cinco componentes: el sensor que recoge y digitaliza los datos, los algoritmos de proceso de los datos adquiridos, un dispositivo de almacenamiento, un algoritmo de coincidencia que compara la información biométrica adquirida con la almacenada en la base de datos y por último la toma de una decisión en base a la respuesta ofrecida por el estudio de coincidencias.

Los datos que se recogen como parte de un proceso de identificación biométrica deben cumplir una serie de requisitos: deben ser invariables, al menos durante un periodo suficiente de tiempo, deben ser medibles, unívocos, aceptables desde el punto de vista de la privacidad y, desde este mismo punto de vista, su tratamiento debe ser fiable y respetuoso con la discreción y la intimidad de las personas.

El proceso de identificación biométrica incluye dos fases: la fase de registro, en la cual el individuo entrega una cierta información al sistema de identificación, y que puede ser automatizada mediante el uso de tarjetas magnéticas o RFID, y la fase de verificación del dato biométrico. . Existen tres tipos generales de consultas biométricas: autentificación, en la que el individuo demuestra voluntariamente que es quien dice ser; verificación, que es generalmente un proceso oculto a los interesados y tiene que ver con actividades de vigilancia; e identificación, en el que se recoge información biométrica de un sujeto desconocido para cotejarla con la totalidad de la base de datos disponible y encontrar posibles identidades.

En los procesos de autentificación y verificación se conoce o se estima la identidad del sujeto; se diferencian en que en un proceso el sujeto sabe que está siendo identificado y en otro no. A menudo los términos de autentificación y verificación se usan indistintamente. Esto acarrea no sólo confusión, sino equivocaciones, ya que se trata de procedimientos diferentes. Por el contrario, la identificación es un proceso en el que no se conoce nada sobre el sujeto y se utiliza información biométrica del mismo para localizarlo

cotejando con todas las entradas de información disponibles en una base de datos.

4.4.3. Aplicaciones del control biométrico

El control biométrico de personas tiene aplicaciones en muchos campos, la mayoría de ellos relacionados con la seguridad y la vigilancia. En casi todos los ámbitos a los que se ha extendido el discurso de «la guerra contra el terror», y éstos son numerosos desde el comienzo del nuevo milenio, se han desarrollado procedimientos para utilizar biometría informática como herramienta de control de acceso y control de seguridad.

En lo referente al control de acceso, bajo este epígrafe se incluirían las medidas destinadas a no permitir el uso de armas, el acceso a bases de datos, oficinas, almacenes y cualquier otro espacio, así como computadoras o cualquier tipo de dispositivo electrónico, a personas que carecen de una autorización expresa. En estos casos suele emplearse la identificación de las huellas dactilares (que contienen entre 50 y 200 puntos únicos) o el reconocimiento de iris (con más de 200 puntos que ayudan a la identificación).

Para gestionar el control de acceso, aunque esta

aplicación está mucho más extendida en el ámbito de la vigilancia masiva, también sirve el reconocimiento facial. Un ejemplo de estos sistemas de reconocimiento facial (basados en las medidas de la posición de nariz, boca, distancia entre los ojos y la altura de los mismos) es el desarrollado en la Universidad Rey Juan Carlos de Madrid, que permite la identificación en tiempo real y de forma totalmente transparente de los individuos, que ni siquiera sabrán que están siendo vigilados.[67] Estos sistemas están pensados para ser utilizados en aeropuertos, como el aeropuerto de Barajas, donde el sistema de la Universidad Rey Juan Carlos ya ha sido probado con éxito (aunque aún no está instalado).[68]

Es curioso que lo que se presenta como una gran ventaja, la capacidad de vigilar en tiempo real y de forma transparente al individuo, sea desde el punto de vista de la privacidad el mayor problema.

4.4.4. Biometría y privacidad

Una última cuestión acerca de la identificación biométrica nos llevaría a analizar la disyuntiva existente entre lo tecnológicamente viable y lo socialmente deseable.

Qué hay de ética en la identificación biométrica y qué hay de legitimidad jurídica. ¿Respeta nuestra privacidad? La pregunta no tiene una respuesta demasiado sencilla, ya que la tecnología de identificación biométrica no se puede eliminar. Está inventada y la solución a una posible violación de nuestra privacidad no pasa por hacer oídos sordos a esta realidad, sino por regular estrictamente los usos que de ella se deben hacer. Estas limitaciones deberían obedecer tanto a la ética de respetar la intimidad de las personas como a lo socialmente deseable para el correcto funcionamiento de la democracia, que es permitir un cierto grado de anonimato.

La identificación biométrica viene de la mano de una promesa: seguridad física para nosotros y seguridad comercial para nuestras transacciones. Bajo el brazo esconde una amenaza para nuestra privacidad que a menudo no se menciona. La defensa frente a esta amenaza contra la privacidad no es tecnológica, que nunca lo es. La defensa pasa por desarrollar un entorno legal apropiado en el que quede claro para qué tipo de acciones se podrá exigir identificación biométrica y para cuáles no, así como los usos permitidos y prohibidos de los datos personales recogidos durante el proceso de registro, ya que toda identificación

biométrica afecta al anonimato y a la privacidad, tan importantes para una sociedad libre. Por tanto, se debería aplicar estrictamente el principio de proporcionalidad, de tal forma que este tipo de identificación sólo se use cuando sea verdaderamente necesario y su implantación compense los riesgos.

Especialmente interesantes resultan dos cuestiones que deben tenerse muy en cuenta cuando se habla de la utilización de identificación biométrica: en primer lugar, la necesidad de eliminar los datos en el preciso momento en que dejan de ser necesarios, y esto podría incluir la eliminación de los registros de acceso tan pronto en cuanto ya no sean necesarios; en segundo lugar, la necesidad de restringir a los casos altamente excepcionales, y no permitir en tanto sea posible, la utilización de sistemas capaces de registrar información del individuo sin conocimiento por parte del mismo. El problema es que en la actualidad el uso de estos sistemas puede dar lugar a abusos con bastante facilidad, y no existen salvaguardas suficientes para los ciudadanos.

La verdadera cuestión en lo referente a la biometría es si ésta constituye una salvaguarda de nuestros derechos o

una violación de los mismos. ¿Aumenta nuestra seguridad o sirve en bandeja una caza de brujas? Lo único que puede hacer que esta tecnología sea algo válido en nuestra vida diaria es encontrar un equilibrio, regido por el principio de proporcionalidad, que impida eficientemente los abusos que en la actualidad se pueden cometer. Asimismo, este equilibrio pasaría por fortalecer el cifrado de la información de los usuarios y por llevar a cabo una catalogación eficiente de los datos para evitar errores de asignación entre información y usuario, algo demasiado común actualmente. Sin todo esto, esta tecnología conlleva más riesgos que beneficios, pero como no es probable que caiga en desuso sin más, no queda otro camino que regular eficazmente las situaciones en las que será exigible una identificación que respete nuestro anonimato y nuestra privacidad. Una vez más la solución no pasa por rechazar plenamente la tecnología, sino por adaptar la ley para que ésta respete nuestros derechos.

Base de datos policial de ADN

El poder identificativo de las medidas biométricas tampoco ha escapado al uso policial. En un uso incipiente en la mayoría de Estados de nuestro entorno, las bases de datos

policiales que incluyen información genética personal pretenden extenderse al conjunto de la población.

En Reino Unido se estima que más de cuatro millones de ciudadanos ya están incluidos en una base de datos de este tipo, y se incluye a treinta mil más cada mes.[69] En España se aprobó un proyecto similar a principios de 2007 y esta base de datos, concebida inicial y teóricamente para incluir a criminales, comenzó a operar en el mes de noviembre de 2007.[70] En Francia también existe un plan similar, pero ha suscitado un debate en la sociedad, que se muestra bastante crítica con «la tentación del fichaje genético masivo»[71] e incluso han surgido campañas ciudadanas en contra del mismo, como la de *Touche pas à mon ADN.*[72]

En España, lamentablemente, el debate no ha trascendido a la opinión pública, ni para bien ni para mal. Nadie se ha enterado de que esta normativa ha sido aprobada, aunque la teoría dice que es obligación de los políticos informar a la gente de las medidas que se adoptan, para legislar de frente y no de espaldas. Es misión de los políticos garantizar que la gente comprenda cómo les están gobernando. Ahí quedará abierto el banco de datos de ADN

de los ciudadanos, a la espera de que se impulse desde el poder un rediseño del contrato social, algo a lo que dedicaremos unas líneas más adelante. La creación de bases de datos con información genética de todos los ciudadanos por imposición gubernamental es contemplada por algunos autores como la mayor amenaza existente para la privacidad.[73]

Inseguridad en la identificación biométrica

La inseguridad de la identificación biométrica tiene un doble vértice: por una parte, toda tecnología de seguridad tiene un cierto grado de vulnerabilidad; por otra, la creencia de que un método de seguridad es infalible hace que sea difícil detectar cualquier vulneración, debido a la falta de preparación para dar una respuesta que suele haber en estos casos.

Desde la duplicación de huellas dactilares y la fabricación, al más puro estilo *Gattaca*, de moldes plásticos[74] hasta la más directa y doliente amputación del dedo completo para robar un coche usando las huellas, como sucedió en Tailandia en el año 2005,[75] las medidas biométricas han demostrado ser del todo inseguras para

garantizar nuestra identificación.

No menos polémicas son las bases de datos con información biométrica, como las bases de datos con información genética, que pueden tener un alto porcentaje de entradas erróneas o mal asignadas. Sobre el problema que supone que en una base de datos supuestamente infalible exista una entrada equivocada es fácil reflexionar: ¿querría usted que por culpa de una entrada con un nombre mal escrito o con una información que directamente ha sido mal asignada se le culpara a usted de algo que hizo otra persona? El delito del que le podrían culpar erróneamente puede ser tan inocente como una multa de tráfico o tan grave como un asesinato múltiple. El carácter supuestamente infalible de estas bases de datos complica las alegaciones y la búsqueda de una defensa efectiva. En cuanto a la posibilidad de que cientos de miles de entradas de la base de datos estén mal asignadas, como sucede en la base de datos de ADN de Reino Unido, mejor no pararse a pensar; resulta grotesco.[76]

Otro problema es que la identificación biométrica acarrea concomitantemente el conocimiento exacto de la ubicación de las personas en todo momento, algo que

vulnera completamente el derecho constitucional a la intimidad. Con la identificación biométrica, nuestro cuerpo -bien su anatomía o bien nuestra manera de movernos- se convierte en contraseña y clave de acceso a nuestra vida diaria (desde la puerta de casa hasta la del despacho, nuestra autentificación en la tarjeta de crédito o en nuestro correo electrónico). Pero, por obvio que parezca, hay que mencionar que en todos estos casos nuestro cuerpo debería ser tratado como un dato personal. De nada sirve implementar un sistema de identificación unívoco si luego esos datos no se protegen adecuadamente y no se tratan con el rigor que exigen los datos personales. Se los debería tratar, de forma inflexible, de conformidad con lo establecido por la Ley Orgánica de Protección de Datos en materia de protección de datos personales.

4.5. TCPA (DRM a nivel de hardware)

Las siglas TCPA corresponden a la Alianza para una Plataforma de Computación Fiable (Trusted Computing Platform Alliance, en inglés) y son un completo eufemismo de lo que la propuesta de esta alianza de fabricantes representa para la población. Aunque pudiera parecer que este asunto es más propio de la lucha por poner coto a los

excesos de la propiedad intelectual, la gestión digital de restricciones a nivel de hardware es un asunto de control tan importante, que lo vamos a abordar en este capítulo. La TCPA es un sistema ideado por los fabricantes para mantener el control total de los dispositivos que producen y para ponerlo en práctica crearon un consorcio empresarial que permitiera desarrollar una tecnología de control que sirviera para todos ellos, ahorrando costes. Dicho consorcio recibió el nombre de Trusted Computing Platform Alliance.

Una de las formas más importantes de control que se está tratando de implantar en la actualidad es la *restricción digital de derechos* a nivel de hardware. Todos conocemos de forma más o menos somera lo que es la gestión digital de restricciones (DRM) a nivel de software, pero este nuevo sistema es diferente. El DRM a nivel de hardware significa que todo componente de una computadora llevará empotrado un pequeño programa que verificará qué se puede y qué no se puede hacer con él y, muy probablemente, otro programa que se encargará de avisar al fabricante en caso de que se produzca un uso no autorizado del hardware. La TCPA es un control y, como tal, es una imposición de una parte (fabricantes de hardware) a

otra (la población).

A mediados de los años noventa, con el endurecimiento de las leyes de derechos de reproducción para favorecer a los editores, los fabricantes de hardware concibieron el sueño de convertirse ellos mismos en los destinatarios últimos de ese favor legal, para lo que debían o bien convertirse en productores de contenidos, o bien convertirse en un control necesario al que todos los contenidos deban someterse. La TCPA representa ese tipo de control. No es algo que sorprenda: igual ambición desarrollaron compañías de telecomunicaciones como *Nokia*, o de otros ámbitos, como *Nielsen*, aunque en este caso se proponga un sistema de marcas de agua[77] que si no se usa adecuadamente conlleva riesgos para nuestra privacidad.[78] El objetivo es convertirse en el certificador y guardián del uso permitido que se da a todo tipo de contenidos y software, con todo el poder de control que eso confiere.

La realidad es que todos quieren ser el nodo necesario, y por eso todos buscan convertirse en productores y transmisores de contenidos, ya que el progresivo endurecimiento de las leyes de propiedad intelectual hace que esta actividad sea algo sumamente

lucrativo; una tendencia que, pese a ser enormemente impopular, no tiene visos de cambiar en lo que respecta a la legislación en los próximos años. Aquel que tenga la posibilidad de controlar los contenidos y datos, así como de ejecutar el software que los interprete, tendrá un poder enorme. Eso es lo que persigue la TCPA.

4.5.1. A quién obedecen los dispositivos

Lo cierto es que la expresión «computación fiable» no puede ser más desafortunada si la examinamos desde cualquier punto de vista que no sea el del fabricante. Un dispositivo no podrá ser nunca fiable si existen una serie de directrices que le indican qué me debe permitir y si hay una serie de órdenes que me delatan al fabricante si decido hacer un uso del mismo que el fabricante no había previsto. Un dispositivo informático no puede ser fiable para mí si no soy yo quien ostenta el control del mismo. Si el dispositivo que he comprado y pagado con mi dinero consulta todas mis peticiones con el fabricante antes de decidir si las ejecuta, ¿a quién pertenece el dispositivo? ¿A quién obedece?

La TCPA pretende desarrollar un sistema en el que solamente el software que presente una determinada

credencial, la firma de un fabricante reconocido y aprobado por el consorcio, pueda ser ejecutado en una computadora. Esto tiene graves consecuencias para la competencia en un mercado libre y, lo que es más importante, tiene graves consecuencias para la libertad de decisión de las personas que usan las computadoras. La excusa esgrimida por la industria para justificar tamaña aberración es, como no podía ser otra, la seguridad, ya que aseguran que de esta forma se evita la ejecución de software maligno como virus o software espía.

Lo que no te dicen, claro está, es que de esta forma también se impide la ejecución de todo software que no tenga el visto bueno del fabricante. Podrían impedirte ejecutar tu propio software si no pagas antes una licencia de ejecución, por ejemplo. Y podrían controlar qué archivos pueden ser cargados con el software que han aprobado, de forma que sólo se puedan ejecutar archivos con una credencial especial. Esto, que podría parecer muy lejano, ya está entre nosotros: los dispositivos de vídeo de alta definición, HD-DVD y Blu-ray, incorporan este tipo de restricciones. Aunque no han sido todo lo restrictivos que podían haber sido, el fabricante puede deshabilitar un

dispositivo si éste ha sido modificado y puede deshabilitar toda una serie de dispositivos si descubren que alguno de ellos ha sido utilizado para extraer de ellos la credencial de seguridad que permite la decodificación de estas películas.[79]

Aunque no es probable que se vaya a adoptar una medida tan impopular a corto plazo, no hay que olvidar que el sistema ha sido diseñado para que exista dicha opción y su sola existencia debería suscitar nuestro rechazo. Si necesitas un motivo importante para no comprar estos dispositivos, éste debería ser suficiente.

Hay quien vaticina que si los fabricantes se deciden a implantar masivamente mecanismos de computación fiable en sus dispositivos, se llegará a una especie de edad oscura digital en la que el progreso se detendrá en seco. Y hay también quien cree que esto generará el nacimiento de un mercado negro de componentes informáticos sin la «letra escarlata».[80] Incluso hay quién piensa que un movimiento de *hardware libre* hará frente a este oligopolio. Yo soy más pesimista. El consorcio de la *TCPA* incluye a los mayores fabricantes de hardware del mundo; si nadie los frena con la fuerza de la ley, será difícil competir en tecnología y medios de desarrollo.

Existen grupos que pretenden lanzar un movimiento de hardware libre, similar al que ya existe en el mundo del software. Ésa sería una gran noticia, pero parece altamente improbable. En palabras de Eben Moglen, «hardware libre es conseguir que los dispositivos obedezcan a sus compradores. Asegurarse de que el hardware responde a la persona a la que pertenece y no a la gente que envía flujos de información a través de ellos».[81] Eben Moglen es optimista sobre la victoria del movimiento de hardware libre, pero se muestra prudente sobre la consecución de la misma. El desarrollo de software requiere bastante conocimiento de programación, pero los requisitos económicos para comenzar a programar son muy pequeños: una computadora no supone ahora mismo una barrera excluyente si lo que queremos es desarrollar software. El desarrollo de hardware, sin embargo, requiere alta tecnología, cuyo precio es muy elevado. Actualmente, no todo el mundo puede colaborar desde su casa para fortalecer. Aunque pronto podremos fabricar todo tipo de utensilios de baja tecnología con nuestras impresoras digitales tridimensionales, éstas son incapaces de fabricar microprocesadores de alta tecnología. No parece que movimientos como *fab@home*[82] y las comunidades en torno

al *fabbing* puedan generar a corto plazo un equivalente en hardware al movimiento por un software libre.

Hoy por hoy para luchar contra la TCPA, la dictadura del oligopolio del hardware, sólo nos sirve, como en otros aspectos comentados a lo largo de este libro, la ley. La ley debe impedir que se incorporen este tipo de controles en los dispositivos, en defensa de la libre competencia y sobre todo en defensa de la libertad de expresión y comunicación de todos. No parece tarea fácil, ya que los partidos políticos, que no dejan de ser un oligopolio, parecen inclinarse habitualmente hacia el lado de este grupo de empresas de hardware (otro oligopolio), pero ése es el reto: conseguir que los políticos elaboren y aprueben leyes que garanticen nuestra libertad.

4.6. Control utilizando Internet

En un mundo que utiliza Internet para todo, la libertad de la red se convierte en una herramienta de máxima importancia. Por supuesto, también en este ámbito hay muchas personas que luchan por la defensa de nuestras libertades. Existen numerosos movimientos y asociaciones, quizá muchísimos, y sólo unos pocos encuentran un eco

social que haga justicia a la relevancia de sus esfuerzos. Sin duda, cuando hablamos de Internet esta relevancia se ve superada tan sólo por los asuntos relacionados con el *copyright*, que por otra parte son muy paralelos al control de la red.

Aunque existen diferentes métodos para vigilar la red, como el rastreo masivo de páginas web (a la manera que lo hacen rutinariamente los buscadores) o, si se tiene el acceso a los registros de tránsito de datos, el análisis del tráfico de información desde, y hasta, una determinada IP, no existen formas eficientes de controlarla. Numerosos gobiernos intentan impedir que la población acceda a determinada información interponiendo filtros y cortafuegos que hagan de barrera, pero, debido al propio diseño de los protocolos que gestionan la red, éste no es un método eficiente de control y, eventualmente, acaba siendo vulnerado. El resultado es que las personas acaban accediendo a la información, y fuera del control al que se las intentaba someter (aunque existe una gran posibilidad de que no escapen a la vigilancia mencionada al principio de este párrafo). Sin embargo, el control de la red, actualmente inabordable, podría ser fácil de conseguir mediante la

modificación de algunos de los principios que la rigen en la actualidad: de esta forma, rediseñar la red sería una forma de hacerla controlable. El control actual de la red no se centra tanto en el bloqueo de acceso como en el análisis de acceso a una determinada información, así como el rastreo continuo de la nueva información que aparece en ella. Como impedir el acceso es inviable, se persigue detectar ese acceso y penalizarlo con posterioridad.

4.6.1. La neutralidad de la red

Por cuestiones de su propio diseño, la red es bastante caótica en su comportamiento. El sistema distribuido está diseñado para asumir el bloqueo de un nodo en la red sin que el resto deje de funcionar, posibilitando el salto de ese bloqueo. Esto podría cambiar si algunas de las características esenciales de la red fueran modificadas. De estas características la más amenazada es la que impide que se penalice a unos nodos de la red frente a otros, haciendo que todos los nodos sean igual de accesibles e impidiendo que se bloquee parcial o totalmente el acceso a alguno de ellos. Esto último es algo necesario para que la red siga siendo un sistema distribuido y se conoce como «neutralidad de la red». Se dice que la red es neutral porque no bloquea ni

prioriza el acceso a ninguno de sus nodos: todos son tratados de igual forma.

Eliminar esta neutralidad que caracteriza el actual diseño de la red es la forma más visible de control de la red. No respetar la neutralidad de la red es ilegal en España, ya que atenta contra la libertad de expresión; está considerado censura. El bloqueo o limitación de las conexiones en redes de pares (p2p) viola este principio, y también es ilegal en España, aunque la obtención de pruebas reales (más allá de la evidencia -no achacable de forma necesaria a un bloqueo del proveedor- de que tu conexión p2p nunca sobrepasa una determinada tasa de transferencia) es tan complicada, que resulta difícil impedir que el proveedor actúe de esta forma.

Este tipo de censura funciona (con muchos problemas) en muchos países como China, Tailandia o Marruecos, pero ha funcionado temporalmente incluso en España, cuando Telefónica impidió temporalmente el acceso a la web de la (por entonces legal) asociación independentista vasca Batasuna, hecho que fue denunciado en medios independientes como Nodo50 o Indymedia;[83] según algunos autores, la orden pudo provenir del gobierno de España.[84]

Exigir que en un futuro se siga respetando la neutralidad de la red es pedir una mínima garantía de libertad de expresión. Sin embargo, se está produciendo un importante debate entre los poderes políticos y económicos, lo que amenaza con modificar este principio básico. Se pretende acabar con la era de las «tarifas planas», subastando la priorización de tráfico: cuanto más pagues, mayor prioridad tendrás; visto de otra forma: si no puedes pagar, serás bloqueado constantemente. Se trata de una negociación agresiva por parte de los proveedores de Internet, que quieren cobrar dos veces por un mismo servicio. Un caso tipo: el de una persona que quiere ver una página web; se cobraría al usuario por poder acceder (esto ya lo hacen y es totalmente lógico) y a la web por poder ser accesible para esa persona. Sin olvidarnos de lo desafortunado del término: si una parte de la cola es priorizada arbitrariamente, otra parte de la misma está siendo retrasada con la misma arbitrariedad.

La imposición de un pago para asegurar que tu web sea accesible pone en serio peligro la red tal y como la conocemos ahora. Las conexiones p2p tendrían que desembolsar este nuevo pago para asegurar que van a estar

permitidas, las webs independientes tendrían que pagar también. Y para colmo, este pago podría ascender exponencialmente, ya que las grandes empresas podrían aumentar el precio a pagar por este concepto como medida eficaz para eliminar la competencia (de todas aquellas pequeñas empresas que no podrían pagar, por ejemplo, lo que Google, Amazon, Microsoft o Fox News estarían dispuestas a pagar).

¿Quieren que la red se convierta en una especie de televisión modernizada que sólo ofrecerá un número limitado de servicios proporcionados por un número limitado de proveedores? ¿Volverían a tener sólo dos canales de televisión y verse obligados a ver lo que éstos ofrecen tras haber probado la televisión por satélite? Por supuesto que no, pero ése es el peligro de eliminar la neutralidad de la red: silenciar todas las opiniones minoritarias. En un mundo digitalizado que utiliza la red para todas y cada una de sus actividades diarias y que lo va a hacer aún más profusamente en los próximos años, garantizar la neutralidad de la red equivale a garantizar la libertad de expresión, la libertad de asociación y la libertad de reunión en el mundo libre actual.

4.6.2. Minado de datos

Ya hemos mencionado que el propio diseño de la red hace muy difícil controlar la difusión de un mensaje a través de la misma. Eso tiene una consecuencia inmediata: para controlar la red en la actualidad lo más útil no es tratar de bloquear el mensaje, sino averiguar quién lo difundió y penalizarle por ello. La filosofía de vigilar y castigar heredada de la vigilancia panóptica se aplica también a la red. En este caso concreto, al análisis de los contenidos y del tráfico de la red para averiguar información sobre las personas y sus actividades se le denomina minado de datos.

La cantidad de información almacenada es enorme y no para de aumentar. La información analizable comprende diferentes ámbitos, que van desde toda lo disponible en Internet hasta registros de compras pagadas con tarjeta. El minado de datos sirve para extraer relaciones entre esos datos que permitan obtener un perfil más completo de una persona como fruto de esa combinación.

Para obtener un perfil preciso de una persona estudian no sólo sus opiniones, sino los productos que consume, la frecuencia con que los consume, así como sus comercios preferidos. En los últimos años, con la eclosión de

la web, sucede que a menudo esta información es pública y nosotros mismos la hemos publicado previamente. Por eso para vigilar la red se requiere una vigilancia analítica capaz de rastrear una cantidad de información gigante, conocer todo lo que se publica en la red y ser capaz de vincularlo a una persona o un tema. Eso es el minado de datos: recorrer los vastos pasillos de Internet recopilando dosis de información respecto a un tema concreto y ser capaz de ensamblarla de forma que se obtenga un retrato de aquello que se busca, ya sea una persona o una actividad.

Web 2.0, los voyeurs y la privacidad

Se conoce como web 2.0 a todo un conjunto de herramientas que facilitan la publicación de contenidos en la web. Sin embargo, la expresión *web 2.0* es más fruto de un interés mercadotécnico que de un verdadero cambio en la relación con la web, ya que la web siempre la hicieron las personas y prueba de ello es que navegadores antediluvianos como Amaya y Netscape eran a su vez editor y navegador web.

En general, las redes sociales de toda temática y los blogs son los dos puntos fuertes de lo que se conoce como

web 2.0. El uso (y sobre todo el abuso) de este tipo de herramientas facilita la labor de minado de datos acerca de nuestra persona, ya que supone una fuente inagotable de información sobre nosotros. Hay una componente que va a diferenciar este tipo de problemas de privacidad de los generados en otros contextos: la voluntariedad. En la web 2.0 somos nosotros los que decidimos participar y esa capacidad de decisión lo es todo. Podemos matizar que participamos para tener un sentimiento de pertenencia a un grupo de personas y que en cierta medida estamos condicionados, pero el hecho final es que somos nosotros los que damos el paso definitivo.

Existen un número creciente de redes sociales, y a menudo en una red social se puede saber sobre nosotros qué webs visitamos y cuáles nos gustan, como en del.icio.us; qué música oímos y cuál es nuestra preferida, como en Last.fm; o quiénes son nuestros amigos, como en Facebook. Es habitual que en nuestro perfil pongamos un enlace a nuestro blog o a alguna otra red social que permita seguir extrayendo información sobre nosotros; y también es posible saber qué temas nos interesan y qué opinamos al respecto, como en nuestras páginas personales.

Es razonable pensar que los problemas derivados de una sobreexposición de nuestra vida íntima debido a la web 2.0 no son tan graves como los problemas derivados de la videovigilancia o la inclusión de chips RFID en nuestros documentos oficiales; al fin y al cabo nosotros decidimos poner esa información en la red. Eso es cierto en gran medida y procuraré no entrar a debatir si estamos socialmente obligados a participar en ella para no sentirnos excluidos, para gozar de un sentimiento de pertenencia a un grupo, algo heredado de nuestro carácter social y contra lo que a veces es difícil luchar.

En cualquier caso, no es menos cierto el hecho de que el poder atribuir el origen del problema a nuestra propia persona no elimina el problema, más bien nos deja sin culpables a los que gritar con los puños cerrados. Y es que lo que nosotros creemos inocuo podría quizá volverse en nuestra contra. Criticar a nuestra empresa puede ser un problema si no medimos las palabras y se nos identifica, pero también el simple hecho de contar detalles de nuestra vida en la red puede suponer un problema. Todo lo que está en la red se puede leer. De hecho, podemos afirmar que todo lo que ponemos en la red lo ponemos precisamente para que

sea leído, incluso cuando aplicamos filtros de acceso. Pero es cuestión de tiempo que los controles que ponemos para filtrar el acceso a nuestra información acaben rotos. Quizá en nuestra próxima entrevista de trabajo, nuestro entrevistador podría saber sobre nosotros más cosas de las que querríamos que supiera.

Autocontrol en la web social

A la hora de publicar en la red debemos reflexionar sobre ello y publicar solamente aquella información que estemos seguros de querer publicar. A menos que estemos completamente seguros de lo que hacemos, no deberíamos poner información personal en la red ni vincularla con nuestra identidad física.

Si en algún momento una autoridad nos exige alguna información, sin duda deberemos facilitarla y conseguir una ocultación... faraónica. Al vivir en democracia, como ocurre actualmente en España, quizá no haya que buscar las últimas consecuencias que para nuestra integridad y nuestra libertad pueda tener el participar en la web social. Pero ello no significa que estemos obligados a firmar con nuestra identidad todas y cada una de las cosas

que colocamos en la red. De hecho, no es en absoluto recomendable si queremos evitar que cualquiera que busque nuestro nombre en la red sepa todo lo que hacemos por ahí, si queremos mantener un mínimo de intimidad.

La privacidad en la web 2.0 va precisamente en la línea de controlar quién puede saber qué sobre nosotros. El verdadero factor diferenciador con respecto a los sistemas de vigilancia masiva es que el control recae sobre nosotros. Hagamos valer esa diferencia y usemos la web con prudencia.

4.7. Fuera de control

De todo experimento de monitorización se puede extraer una conclusión: si el individuo sabe que está siendo observado, modificará su conducta. Es el fundamento que reside y confiere su fuerza al ideal panóptico de Jeremy Bentham, que preside no sólo las políticas de control, seguridad y defensa actuales, sino la ética social y laboral de nuestro tiempo. El miedo a ser descubiertos, penalizados o denunciados nos obliga a trabajar sin parar, a no ser descorteses con nuestros semejantes, a actuar cívicamente.

En 2006 se llevó a cabo uno de estos experimentos

panópticos en la Chaos Communication Conference entre los asistentes a la misma que quisieron participar. El experimento no empleó videocámaras, sino tecnología RFID.[85] Los voluntarios recibieron un emisor RFID activo y el auditorio fue equipado con más de una treintena de receptores capaces de indicar al sistema dónde estaba cada uno de ellos en cada momento: en la sala de conferencias, en el pasillo, en el recibidor, fuera del edificio. Para hacerlo aún más sencillo, el sistema publicaba en la red automáticamente la posición de cada persona, que se podía seguir mediante un canal RSS.

La conclusión a la que llegaron tras el experimento fue que «la mayoría de los usuarios ni siquiera notó que lo llevaban e incluso algunos lo olvidaron en casa al segundo día», pero «algunos tenían una sensación como de Gran Hermano y pudimos observar cómo algunos decidían a qué conferencias acudir siendo conscientes de que los estaban observando».

Aunque la primera conclusión parezca inocente no lo es: estar bajo vigilancia sin ser consciente de la misma no es nada inocente. La segunda conclusión del experimento es la bomba panóptico-conductista que todos conocemos: la

conciencia de estar bajo vigilancia es un condicionante del comportamiento.

Parece probable que en la CCC la mayoría de usuarios que se adhirieron a esa iniciativa estaban mucho más interesados en clonar e investigar con esas tarjetas que en llevarlas para ser identificados, pero lo que tanto ellos como cualquier otro no podrá negar es precisamente el resultado obtenido de esta prueba: el sentirnos vigilados modifica nuestra conducta. El asistir a una charla para no ofender al conferenciante o evitar ser recriminado más tarde sólo porque uno sabe con total seguridad que se sabrá que no ha estado es una de las peores consecuencias del control social excesivo y de todas las tecnologías que proporcionan dicho control: el poder para obligarnos a hacer cosas que de otro modo no haríamos.

Ése es el motivo por el cual es necesario el poder para mantenernos fuera de control, desconectados del sistema, escondidos del alcance de sus sensores, sean del tipo que sean. Si las tecnologías que permiten localizar personas u objetos, o rastrear personas en la red, pudieran ser desconectadas a voluntad, no serían realmente negativas. Podríamos disfrutar de todos sus beneficios

cuando así lo requiriéramos, sin los problemas derivados del descontrol de la misma.

El problema es que estos sistemas, en especial la videovigilancia y los chips RFID, no se pueden desactivar con facilidad. En ocasiones se ignoran premeditadamente estos asuntos o, en caso de que no sea posible ignorarlos, se nos dirá que el problema en sí no existe porque los dispositivos se pueden desconectar fácilmente. La realidad no es ésa, sino que no es posible desconectarse a voluntad. En algún momento perdimos ese derecho.

4.7.1. Grabándolo todo en todas partes

Una de las consecuencias del abaratamiento de la tecnología, del desarrollo de las redes y del aumento y abaratamiento de la capacidad de almacenamiento de información es que actualmente todo queda registrado en alguna parte.

Cuando decimos esto no nos referimos únicamente al Proyecto de Ley de conservación de datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones [86] que sirve para trasponer la Directiva Europea de Retención de Datos de Telecomunicaciones, sino

que vamos mucho más allá: no se trata sólo de que la ley obliga a almacenar una serie de datos de toda comunicación (emisor, receptor, mecanismo, hora, dispositivos utilizados). En la actualidad, eso es sólo parte del problema. Si envías un SMS, tu proveedor de telefonía guardará tu número, tu nombre, así como el número y el nombre del receptor, la hora del envío, el medio utilizado. Pero lo más probable es que la persona que recibe el mensaje guarde una copia; quizá esa copia no se borre nunca.

Evidentemente, en un mundo donde los correos nunca se borran, los SMS se guardan de por vida y donde la comunicación gira en torno a la red, algo que aumentará cuando la telefonía convencional acabe su migración a la telefonía sobre IP, todo queda registrado en alguna parte. Las compras del súper se añaden a tu perfil de cliente, los correos que escribes son registrados por el receptor, por el proveedor del servicio (que adapta su publicidad al contenido del correo) y también por tu proveedor de Internet (este último por obligación del Estado).

Existe un problema añadido con la legislación de retención de datos e Internet. Mientras en un mensaje SMS convencional es fácil conocer dónde empieza y acaba el

mensaje, dónde está la información de cabecera y dónde el contenido que no debe ser registrado, en las comunicaciones por Internet esos contenidos son altamente inmiscibles. Es muy difícil diferenciar, en la trama de datos, cuándo estamos solicitando una URL, cuándo estamos recibiendo la información de esa URL o cuándo estamos conectando mediante telefonía IP con alguien y cuándo estamos, efectivamente, hablando. Esto implica que quizá no sea tan factible el almacenamiento aséptico del esqueleto de las comunicaciones sin almacenar también el contenido. Y no es que el almacenamiento de los datos básicos de comunicación (sin contenido) sea inocuo, ya que de ahí se puede extraer una información mucho más detallada de lo que parece a simple vista y que permitiría, por ejemplo, reconstruir completamente nuestra red de contactos, sino que el carácter indisoluble de marco y contenido en las comunicaciones por Internet es un problema añadido en este caso.

El problema es que cuando todo queda registrado en alguna parte, todo es susceptible de ser usado en nuestra contra. No hay que ser excesivamente dramáticos, no estamos hablando de injustos tribunales militares que nos

ajusticien, sino de algo mucho más cotidiano, como una campaña de descrédito de nuestro adversario político.[87]

Esto podría parecer bueno: se podrá juzgar a un terrorista. Pero constituye un acto más de puro teatro de seguridad combinado con un oportunísimo interés por la vigilancia: vigilar a toda la población es una tarea faraónica; se podrá averiguar a posteriori quién planeó qué, pero no se podrá evitarlo. La vigilancia intensiva no evitará los atentados ni sus víctimas. Este sistema es ineficaz para la prevención de atentados, pero es altamente efectivo para la observación de una persona en concreto a la que se quiera atacar para, por ejemplo, desprestigiarla, algo que ya ha sucedido en Estados Unidos.[88]

Por tanto, en lugar de estar más seguros, la vigilancia intensiva nos sitúa en una posición de inseguridad. Simplemente, imaginen que toda esa información está al alcance de alguien que les odie a muerte o, en una situación mucho más mundana, alguien que compita por el mismo objetivo que ustedes (un puesto de trabajo, una victoria electoral).

5. Derechos de reproducción

Parece inevitable en la actualidad hablar de derechos de reproducción y propiedad intelectual siempre que se aborda algún tema, cualquiera que sea, relacionado con Internet, la sociedad digital o la libertad de expresión. También a mí me ha resultado imposible no tratar el tema. Si hubiera que buscar una explicación, ésta sería probablemente la omnipresencia mediática de las empresas que basan su negocio en la existencia y ampliación de la restricción de copia. Discográficas, editoriales, productoras de contenidos en general y sociedades de gestión han demostrado sobradamente controlar a la perfección el «noble» arte de la presión política y mediática. Supongo que

multitud de voces lanzando apreciaciones de toda índole e inmiscuyéndose en todos los asuntos de nuestra vida cotidiana tenían que dar sus frutos. Así que ahora, en todo manual sobre privacidad y control social, también hay que dedicar un hueco a los derechos de reproducción. Allá vamos.

Hablamos de este asunto porque si bien es posible que actualmente el *copyright* no sea en sí mismo una amenaza para nuestra privacidad, no es menos cierto que afecta a nuestra libertad de expresión y que los elementos y las tácticas desarrolladas por la industria para impedir la copia de sus contenidos o controlar a los que copian servirán y podrán ser utilizados, llegado el caso, para impedir la copia de cualquier otro elemento o averiguar quién lo ha copiado, algo que afectaría seriamente a nuestra libertad de expresión.

Los derechos de reproducción o *copyright* constituyen una limitación de acceso a la información y tienen un nombre concienzudamente engañoso, ya que en realidad lo que los derechos de reproducción regulan es la *restricción de copia* o la *restricción de derechos de reproducción*. El *copyright* limita el derecho natural a copiar lo que

poseemos y determina que una obra no pueda ser reimpresa y redistribuida, de forma que el número total de ejemplares se mantenga artificialmente escaso[89] para aumentar su valor nominal.

Como último motivo para justificar la inclusión de este capítulo no hay que olvidar que la cultura es lo que nos ayuda a mantener un espíritu crítico y a forjar nuestra personalidad. No es que quiera decir que «sólo la cultura nos hará libres», aunque ya sea tarde para no decirlo y además esté de acuerdo. Lo que realmente sucede es que el derecho a acceder a la cultura no es el derecho al ocio. La cultura nos forja. El tipo de cultura al que podamos acceder y la cultura a la que decidamos prestar atención y dedicar nuestro tiempo determinará nuestras aficiones, inquietudes, deseos e ideologías. La lucha para relajar las restricciones de copia no es una lucha para poder escuchar música pagando menos: lo que está en juego es el derecho al desarrollo de una personalidad propia con criterios de decisión propios, y para ello es necesario que toda cultura esté disponible de manera que nadie, tampoco el Estado, pueda determinar la cultura y la forma de pensar de las personas.[90]

5.1. El origen

La primera ley de restricción de copia surgirá en Inglaterra como consecuencia de la aparición de la imprenta. La imprenta se introdujo en 1476 y representó un cambio trascendental en la producción cultural: por primera vez la producción cultural conseguía generar riqueza. Aunque al principio este nuevo invento no causó mayores problemas a la monarquía de los Tudor a principios del siglo XVI, fue común la emisión de octavillas y panfletos con mensajes republicanos, políticos y religiosos. La monarquía británica intentó entonces controlar esta opinión discordante mediante la introducción de un sistema censor. El sistema imponía un sistema de licencias de imprenta, sin la cual utilizar una de estas máquinas para fabricar y distribuir mensajes era ilegal. La intención de la monarquía británica de la época al promulgar esta ley no era otra que la de protegerse a sí misma evitando la aparición de panfletos y octavillas con mensajes republicanos y contrarios a la política del rey.[91]

Pese a su origen censor, la legislación sobre esta materia pronto evolucionó para que, además de servir como medio de control, también protegiera la inversión de los

editores en el creciente negocio editorial. La idea era construir un mecanismo jurídico que asegurase al impresor unos beneficios económicos que compensasen, cuando menos, las ingentes cantidades de dinero necesarias para la impresión. La solución fue otorgar al editor un privilegio exclusivo sobre la explotación de la obra frente a todos los demás impresores: lo que se conoce como restricción de copia o *copyright*. Pero eso no fue hasta mucho tiempo después, hasta el año 1710 con la entrada en vigor del Estatuto de Ana, denominado así por la reina que ocupaba el trono en ese momento, y al que se considera el primer texto legal que incluía la restricción de copia como un privilegio para favorecer a los editores.[92]

La idea del *copyright* no existía en la antigüedad, y era frecuente que los autores copiasen fragmentos -a veces extensos- de otros autores en sus propias obras. Esta copia, lejos de suponer un delito o un problema, ha resultado ser muy útil, ya que es la única responsable de que obras de autores clásicos griegos y romanos hayan sobrevivido hasta nuestros días. El *copyright* se inventó para ser utilizado en el ámbito de producción de libros en una época en que éstos sólo se podían copiar en una imprenta, y para ello hacía falta

dinero. Un matiz importante, y que los defensores de un endurecimiento de la legislación que fortalezca la restricción de copia parecen haber olvidado, es que el propósito supuesto de esta restricción era (y en teoría es) promover el progreso, no recompensar a los autores, pues estos ya eran recompensados con la venta de sus obras una vez eliminada la competencia desleal.

El entorno actual, tanto en lo que se refiere a la producción -mucho más barata ahora- como a la legislación sobre restricción de copia -mucho más restrictiva en la actualidad-, es radicalmente diferente al que se encontraban los editores de libros hace un siglo y medio.

5.2. Derechos de autor y derechos de reproducción

Conviene detenerse el tiempo suficiente en estos conceptos para diferenciarlos, ya que en los últimos años se han mezclado intencionadamente hasta la saciedad. Los responsables de tan lamentable mezcla no son otros que las empresas y sociedades que tienen como modelo de negocio la producción y venta de contenidos de todo tipo (noticias, libros, música, vídeo) y que recurren a la generación

artificial de escasez para aumentar el precio final de éstos. Estas empresas pertenecen mayormente al sector del entretenimiento (discográficas, estudios cinematográficos, sociedades de gestión).

Más allá de dicha confusión, los derechos de autor y de reproducción son cosas diferentes. Los derechos del autor tienen carácter moral y se resumen en algo tan sencillo y comprensible como el derecho al reconocimiento de la autoría de una determinada obra. Este derecho es básico y, según las leyes vigentes en nuestro país, es además inalienable. Por contra, los temas con los que se suele polemizar en las noticias y que suelen llenar nuestras conversaciones (restricción de copia, canon, DRM) no son conceptos relacionados con los derechos de autor, sino con los derechos de reproducción de una obra, que no son un derecho básico y, de hecho, multitud de obras no están sujetas al mismo. Este libro, por ejemplo, puede ser copiado sin restricciones, pero usted no puede plagiarlo y decir que lo ha escrito. Este libro lo he escrito yo y eso no se puede cambiar; el derecho a copiarlo sí se puede cambiar y se ofrece desde un principio.

La confusión de estos términos no es casual ni

gratuita. Se mezclan como parte de una estrategia de legitimación de medidas restrictivas y excluyentes, como la restricción de copia, que pasa a estar indivisiblemente unida a la inalienable autoría moral de la obra. Pero, ¿es eso cierto?

La confusión total la añade la expresión «propiedad intelectual». Esta expresión es relativamente reciente, y algunos autores sitúan su origen en la década de los sesenta del siglo XX. Otros autores la definen como un oxímoron puro, mientras que otros simplemente preferimos usar un simple ejemplo para deducir que a las ideas y a la producción intelectual no se le puede aplicar una ley de propiedad que sí es válida para otros productos convencionales. Supongamos que yo tengo una fruta y usted otra, si las cambiamos entonces yo sigo teniendo una fruta y usted otra; supongamos ahora que yo tengo una idea y usted otra, si las cambiamos entonces yo tengo dos ideas y usted también tienes dos ideas. De modo que las ideas, lo intelectual, no se pueden medir con las varas de la propiedad material, ya que su naturaleza es distinta. Además, no hay nada más humano que la tendencia a la copia y la modificación de una idea original de otra persona

para mejorarla Es de esa forma como ha avanzado la sociedad: ensayo y error, copia y mejora.

El objetivo de mezclar la restricción de copia con los derechos morales del autor es hacernos creer que la abolición de los derechos que restringen la reproducción de las obras no solo es inviable, sino que es inmoral, mostrarnos la falsa percepción de que un mundo sin *copyright* es un mundo hostil y caótico, lleno de pillajes en el que nadie haría nada porque no existen incentivos. Pero la realidad es bien distinta: en un mundo donde no se restringe el acceso a la información, la necesidad de saquear lo ajeno desaparece. La supuesta falta de incentivos que vaticinan podría ser la antesala de algo mucho más grande: la creación sin barreras, la aplicación directa de nuestras ideas para mejorar lo existente o simplemente adaptarlo a nuestras necesidades. Sin trabas, sin límites legales. El avance social que permite la tecnología digital, optimizado.

5.3. Los sistemas continental y estadounidense

Cuando nos centramos en los asuntos de la propiedad intelectual, la principal diferencia entre la

doctrina anglosajona y la doctrina continental radica en la inalienabilidad de los derechos morales básicos de autoría de una obra. De este modo, en la legislación europea, que otorga al autor un papel central, no se contempla la posibilidad de que una persona cree una obra y sea otra persona la que la firme y reclame su autoría. Esta práctica es ilegal en España y está penada ya se realice con el consentimiento del autor -que podría recibir dinero a cambio de renunciar a esos derechos morales- o de forma violenta, mediante el robo de la autoría de la obra; por contra, está muy extendida en Estados Unidos, donde es habitual ceder la autoría de la obra a la persona o empresa que paga el servicio y contrata al creador. El derecho al reconocimiento de la autoría es, según la doctrina continental, inalienable y el autor no puede ser desprovisto del mismo. Esto sí lo permite la legislación estadounidense, que no otorga la atención central al autor, sino al mecenas. Ambos sistemas penalizan el plagio. En ambos sistemas los derechos de explotación exclusiva han de tener una duración limitada, periodo tras el cual todas las creaciones pasarán a estar en el dominio público, permitiéndose entonces su edición, fabricación (en el caso de las patentes para desarrollos industriales), modificación y mejora por

parte de otros individuos. La finalidad de esta limitación es impedir que una protección infinita bloquee el avance de la sociedad.

Además de las desemejanzas de base, entre estos sistemas hay otra diferencia interesante: la capacidad de sentar jurisprudencia que tienen las sentencias previas. En el sistema estadounidense una sentencia previa sienta un precedente que es difícilmente evitable, mientras que en el sistema continental es habitual que se requieran varias sentencias para sentar un precedente y, además, un juez siempre podrá decidir en otro sentido. Los defensores del sistema continental argumentan que esta propiedad le otorga una mayor capacidad de adaptación a los cambios de la sociedad.

Para el ser humano común, que dista de ser un experto en leyes, la comparación entre ambos sistemas se puede apreciar en aquello que nos ofrecen las leyes que se derivan de una y otra percepción. El sistema norteamericano es mucho más restrictivo y no permite la copia privada como un derecho del usuario, como medio para favorecer al mecenas. Los defensores de las restricciones digitales (DRM) argumentan que son una

consecuencia natural de la manera en que el derecho estadounidense aborda este asunto. Por contra, el sistema europeo es mucho más respetuoso con el ciudadano y le permite realizar copias privadas de una obra para su uso personal o íntimo sin ánimo de lucro. Los defensores del canon o compensación por copia privada argumentan que es una consecuencia lógica de la forma en que el derecho europeo aborda esta cuestión.

La paradoja de esta dicotomía del derecho es que en un mundo gobernado por instituciones supranacionales como la Organización Mundial del Comercio (OMC) y en el que el mercado de producción de contenidos está concentrado, con cuatro distribuidores que se reparten el 85 % del mercado de distribución musical, los sistemas anticopia se distribuyen globalmente, por lo que ignoran el modo en que la legislación de cada Estado aborde este asunto. Podría decirse que esta es otra consecuencia nefasta del Consenso de Washington,[93] que da origen a la mal llamada globalización. La consecuencia es que en tanto nuestra legislación no prohíbe explícitamente el uso de medidas anticopia, porque nuestra visión del derecho no había vislumbrado la existencia de tal posibilidad, esta

imposición viola los derechos derivados de nuestras leyes y nos toca convivir con las peores consecuencias de ambos sistemas jurídicos (*nuestro* canon y *sus* DRM).

Viendo lo que los distintos gobiernos que hemos ido teniendo han legislado en esta materia, que está lejos de practicar el inmovilismo o recortar los derechos de los editores, algunos defensores de la cultura libre, como Pedro J. Canut, consideran que el canon es un mal necesario para evitar la justificación legal de la inclusión por defecto de sistemas DRM. Canut argumenta que en tanto no consigamos modificar la forma en que la legalidad entiende la restricción de copia, abolir el canon equivaldría a dejar pasar el caballo de Troya. Abolir el canon sin reformar paralelamente la ley de propiedad intelectual para adecuarla a la sociedad digital y hacerla más permisiva sería aceptar el sistema estadounidense, mucho más restrictivo y claramente incompatible con el derecho continental y con nuestra constitución.[94]

De modo que a corto plazo, mientras el debate y la influencia política sigan polarizados como lo están actualmente, no parece viable que la situación vaya a mejorar. Sin embargo, la opción que tenemos no es otra que

influir en el modo en que en la agenda pública se trata este tema para que la discusión se enfoque no en torno a los hipotéticos daños sufridos por un colectivo (más que discutible si hablamos de los músicos, que están más demandados que nunca para tocar en directo) sino en torno a la libertad de uso de los conocimientos y la información que adquirimos. Esto es muy importante si queremos que la visión que mejor defiende una cultura accesible para todos vaya abriéndose paso.

5.4. El mito del autor genio

Casi la totalidad de la legislación actual sobre derechos de autor y propiedad intelectual se apoya en un concepto tan arraigado en nuestra mente y tan arcaico, que nunca reparamos en él: el mito del autor genio. Pero la propia calificación de *mito* indica que no existe, sino que forma parte del ideario fantástico común.

El autor genio es el nombre que recibe el concepto que desde los círculos tradicionales de la cultura se nos transmite de lo que es, o debe ser, un autor. El autor genio crea por naturaleza, y crea partiendo de la nada. No necesita formación para crear, es un genio y tiene talento. No

necesita otra cultura anterior, no debe estudiar, ni siquiera es preciso que haya participado antes de la cultura. Esta participación incluye también las leyendas populares o los cuentos de Dickens que le contaban de pequeño.

Sin duda alguna este mito del autor genio servía al propósito para el que fue creado mucho tiempo atrás: engrandecer la figura de los creadores. Y no surgió como una medida proteccionista de la obra creada, sino como la forma más básica de propaganda concebida para enfatizar las diferencias sociales de la época en que surgió: en un tiempo en que la mayoría de la población no recibía educación, o esta era mínima, y debía trabajar desde la infancia es evidente que aquellos que podían dedicarse a la pintura, la escultura o las letras eran unos privilegiados sociales. De ahí que el engrandecimiento de la figura del creador genial que no necesita nada más porque tiene talento no sea más que una operación por la que las clases altas se ganaban la admiración y el respeto de las clases más bajas, generalmente sus lacayos, admiración que de otra manera habrían tenido que ganar por la fuerza.

Lo paradójico es que en una época como la nuestra, en la que las diferencias se acortan y cualquiera dispone de

medios más que suficientes para dar rienda suelta a la creación artística y distribuirla a un coste ciertamente pequeño, el mito del autor genio sobreviva con fuerza. El hecho de que este mito sobreviva de forma tan poderosa se debe, una vez más, a la presión que desde el universo cultural, típicamente desde las empresas editoriales y discográficas, se ejerce para mantenerlo vivo.

En la actualidad, no hay nada menos exclusivo que la capacidad de producir y distribuir creaciones artísticas, al menos en un país desarrollado. Obviamente, no todo el mundo dispone de un taller enorme en el que realizar esculturas ni pintar lienzos del tamaño de la capilla Sixtina, pero sin duda no existe esa limitación en muchos otros ámbitos de la creación cultural: la música, la literatura y el cine requieren cada vez menos inversión técnica y más inversión en formación previa y estudios. El mito del autor genio se desmorona, como no podía ser de otra manera en la era de la remezcla, el reciclaje y los pastiches.

5.5. Los excesos legales actuales

Los defensores de la restricción de copia apoyan sus argumentos en que, sin dicha restricción, no existiría

recompensa a la creación. Esta afirmación es falsa. No vamos a afirmar que actualmente estemos preparados para la abolición de todo derecho de restricción de copia, precisamente por lo que ya hemos mencionado anteriormente sobre el comercio electrónico (los bienes que se compran y se venden son en su mayoría físicos y cuesta dinero producirlos), pero hay una gran diferencia entre eso y afirmar que en ciertos ámbitos no se pueda concebir una reducción drástica de estos monopolios, que su abolición no pueda ser viable en un futuro o que ésta sea inmoral.

La legislación en esta materia está encaminada a restringir el uso que se puede hacer de la información, ya sea cultural o técnica. La legislación de este ámbito, que engloba la protección de obras culturales por una parte y la legislación sobre desarrollos industriales y patentes por otro, concede al autor un periodo durante el cual podrá explotar en exclusividad la creación. Esta medida tiene como finalidad privilegiar al autor para facilitar la generación de un rédito gracias a la creación, si bien lo habitual en la mayoría de casos es que el autor acepte la cesión por vía contractual de los derechos de explotación de las obras.

Para entender el exceso de la legislación actual en

esta materia hay que remontarse al origen del conflicto que se pretende regular con estas leyes. En los orígenes de la legislación sobre restricción de copia no subyace la defensa de los derechos de autor, sino la defensa del avance social: se protegía la inversión del editor no para salvaguardar al autor en sí mismo, sino para permitir que la sociedad siguiera acogiendo a creadores. El problema actual reside en que esta legislación se ha endurecido, de forma que el principal beneficiario ya no es la sociedad, que no consigue más autores de los que habría en su ausencia, sino las empresas que gestionan la distribución de estas creaciones. Se han ampliado los plazos de exclusividad concedidos por la ley de forma abultada (decenas de años tras la muerte del autor) y se ha entrado en una dinámica que amenaza con no dejar de ampliarlos. De esta forma, un privilegio temporal y limitado amenaza con volverse ilimitado, en contra de lo que sería deseable y en contra de la naturaleza misma del argumento que lo sustenta.[95]

Mucha de esta legislación ha perdido sentido en la sociedad digital. Si nos ceñimos a la reproducción digital de obras culturales, el coste de las copias es prácticamente nulo y, con el aumento de las capacidades de almacenamiento y

transmisión de la información, seguirá reduciéndose hasta llegar a cero (ya se acerca bastante). De esta forma, todo el coste de producción recae en la producción del primer ejemplar, pero eso siempre ha sido así. La conclusión es que la producción masiva de copias es infinitamente más barata que antes y se amortiza más rápidamente. Y lo que es peor: limitar artificialmente el número de copias para aumentar su precio resulta poco ético. No menos grave es que el encargado de provocar esta escasez, generada mediante estos monopolios legales, sea el propio Estado.

Quizá no estemos preparados para la abolición total de los derechos de reproducción. Quizá, lo mismo que sucedía con el comercio electrónico, nadie ha encontrado la manera de recompensar adecuadamente a muchos de esos productores de información. Quizá la teoría de la *economía de la atención*[96] no sea completamente aplicable a todos los ámbitos, como a toda la creación literaria -dada la preeminencia del libro físico como formato de lectura-, pero parece seguro que los autores de otro tipo de obras, como las obras musicales, cuyos ingresos se deben mayoritariamente a actuaciones en vivo y mercadotecnia, sí están preparados para asumir el cambio, ya que la demanda de actuaciones

aumenta con la disponibilidad de las obras, como ha quedado demostrado en los últimos diez años con dos hechos paralelos: la aparición de las redes de pares (*peer-to-peer*, o *p2p*) y un incremento sin precedentes del número de conciertos.

A los detractores de la economía de la atención, que dicen que ésta no será capaz de mantener a todos los creadores, quizá se les podría contraargumentar que tampoco todos los que han estudiado periodismo en la universidad han acabado viviendo del periodismo. Está claro que todos no podemos vivir de ser mimos en la calle; si todos quisiéramos ser mimos, tendríamos un problema porque no habría suficientes calles para todos. Pero el problema sería nuestro, no de alguien que, al pasar, decide qué mimo le gusta tanto como para elegir su sombrero y echar una moneda.

En cualquier caso, la no existencia de un modelo alternativo no significa que la marabunta social no pueda responder a la presión, impuesta por los excesos del sistema actual, atacando al propio sistema. Este entorno caótico no es una solución a largo plazo, pero la lógica dialéctica nos dice que ante una imposición de orden brutal, la única

respuesta es la desobediencia. El p2p es, quizá, la anarquía: un sistema sin control y sin nodos con derecho al veto de contenidos. Nadie sabe con seguridad cómo se va a retribuir a los artistas y editores cuya música se transfiere vía p2p, aparte de obtener una mayor difusión con la que potencialmente aumentarán las contrataciones para actuaciones en directo o la creación de obras mediante mecenazgo previo, pero todos saben que los precios y las condiciones impuestas actualmente por los editores no son justos. Anarquía sin nodos. Comunicación de igual a igual.

5.5.1. La restricción de copia y la libertad de expresión

La red facilita enormemente la difusión de mensajes de forma distribuida. Una vez que un mensaje entra en la red, es muy probable que resulte casi imposible detenerlo. Ya hemos mencionado el control en la red y las técnicas de minado de datos que sirven para cotejar diversa información y vincularla a fin de encontrar una relación y obtener un conocimiento nuevo. Hablábamos de como el análisis automático y minucioso que se efectúa de las numerosas bases de datos disponibles permite trazar perfiles personales muy detallados de las personas cuya información estaba en

dichas bases.

Sin embargo, hay quien ve en la restricción de copia y en los parapetos ofrecidos por la propiedad intelectual un medio para censurar información. Éste es el aspecto más conflictivo de la restricción de copia: no es sólo que genere exclusión del acceso a la cultura, sino que la herramienta que hace posible impedir que se copie una determinada canción, hará posible impedir la copia de cualquier otro tipo de información. En este contexto, con el creciente aumento de la cantidad de información recogida en la red y el aumento de nuestra dependencia de los motores de búsqueda que nos permiten bucear entre tan vasta información para encontrar lo que buscamos, es precisamente la presión sobre estos buscadores (para que bloqueen la aparición de ciertas webs en sus resultados) el sistema utilizado para censurar información. Así sucede en China, con la torpe excusa de defender un régimen dictatorial, y así sucede en Estados Unidos., donde so pretexto de una violación de la DMCA (Digital Millenium Copyright Act) se bloquean ciertos resultados de búsqueda. Esto no debería sorprendernos, pues los responsables de la censura en China y en Estados Unidos resultan ser los

mismos; en este caso concreto, Google.[97,98]

5.6. La industria del *copyright*

El cambio de paradigma tecnológico no ha sido aceptado por todas las empresas que directa o indirectamente basan su negocio en los monopolios legales que el Estado les concede aplicando la legislación sobre derechos de autor. La industria del *copyright* no ha sabido adaptarse al nuevo entorno digital, salvo honrosas excepciones, y eso cierra el círculo de la discusión en este ámbito.

A finales del siglo pasado se comienza a fraguar un cambio social tan radical (el coste derivado de realizar sucesivas copias de una obra en formato digital es irrelevante), que amenaza con arruinar los negocios que giran precisamente en torno a la comercialización de esas copias en formato físico. Cuando una copia casera de un disco tiene la misma calidad que el original y me cuesta lo que me vale un CD virgen, que puede rondar los diez o quince céntimos, las personas y las empresas que pretenden vender copias idénticas a mi producción casera, pero a un precio muy superior de veinte euros, tienen un problema

muy grave. Pero este problema es económico y la solución es fácil según las reglas de la libre competencia: si puedo obtener un mismo producto por dos vías, usaré aquella que tenga un menor coste.

Sucede que las grandes empresas son a menudo las mayores partidarias del liberalismo económico (habitualmente excesivo), pero ahora nosotros, la sociedad en general, hemos tomado prestado ese liberalismo económico y, cuando lo aplicamos a la economía del hogar, la solución del problema pasa por dejar de pagar precios desorbitados (desde los dieciocho o veinte euros de un disco compacto hasta los veinticuatro que puede costar una película recién editada en DVD) por una copia que nosotros mismos podemos hacer en casa con un coste marginal. ¿No resulta lógico? Y sin embargo, copiar esa pieza en formato físico no es más que un segundo óptimo, ya que podría dejar de hacer esa copia física y, directamente, almacenar esa obra en formato digital, mucho más versátil, mucho más ligero y que ocupa mucho menos espacio. Y para ser fieles a la verdad, no lo hago siempre. No es que aún haga copias físicas de mis álbumes y películas preferidas, es que sigo comprando álbumes y películas de artistas que me gustan de

verdad.

Sin embargo, la historia no es tan sencilla. Esta industria, en lugar de adaptarse a la situación que la sociedad, la tecnología y el mercado le están imponiendo y gastar parte de su abultado superávit anual en probar y desarrollar modelos de negocio alternativos que le permitan evolucionar y sobrevivir, ha optado por presionar a los gobiernos para que endurezcan las condiciones del monopolio que la legislación les concede. Al mismo tiempo, utiliza todas sus armas propagandísticas para criminalizar el intercambio de archivos y a las personas que lo practican, pero impone condiciones de alquiler y venta controladas por área (por ejemplo en sitios como Amazon.com) que pueden llegar a retrasar muchos meses (en el caso de algunas series, hasta dos temporadas) la llegada del material a otras partes del mundo. Este material podría llegar en minutos y una descarga rápida atraería a personas al servicio de pago. Imponer un retraso en el envío del producto que puede superar el año y culpar a los demás de la aparición de vías alternativas que lo filtran y lo llevan allí donde está uno generando escasez artificial es ridículo, pero es la táctica que está utilizando gran parte de las compañías que se

dedican a este negocio.

Editoriales, discográficas y estudios de cine acuden a las puertas de los despachos de los políticos para ir poniendo, secuencialmente, sus peticiones sobre la mesa. No es algo nuevo: la alianza entre las fuerzas culturales y políticas fue ideada por los partidos comunistas en la década de los cuarenta del siglo pasado y ya sabemos que desde los años sesenta y setenta la industria del *copyright* ha estado metiendo miedo, anunciando el apocalipsis por culpa, sucesivamente, de las grabaciones en cassette, los videoclips, los vídeos caseros, Internet, las grabadoras de CD, etc., y un sinfín de causas que en estos cuarenta años han *aniquilado* las discográficas al menos diez veces.

Y sin embargo, cada año todos y cada uno de los escalones de esta cadena de negocio anuncian nuevos y apetitosos resultados con récord de ganancias. Con ese dinero subvencionan los eventos y apoyan a los grupos de presión empresarial encargados de obtener de nuestros políticos nuevos favores, nuevas vueltas de tuerca a la legislación que apoya su negocio. Y los políticos, prácticamente en todo el planeta, acceden a ello. Como no voy a menospreciar la inteligencia de los políticos de medio

mundo, que generalmente saben muy bien lo que les conviene, la opción que queda es pensar que la legislación en materia de derechos de autor y propiedad intelectual es deliberadamente dañina, deliberadamente ineficaz, deliberadamente injusta. La opción es pensar que los políticos buscan algún beneficio propio con estas leyes. ¿Quizá un poco de control social? Sí, quizá.

5.7. La exclusión

Cuando hablamos de exclusión nos referimos a la exclusión que sufre una parte de la sociedad del acceso a la cultura y los bienes culturales. Esta exclusión tiene consecuencias en todos los ámbitos de la vida y se ve agudizada por las medidas tecnológicas y legales que impiden el libre acceso a la cultura. En una época en que el acceso a la misma se debería haber abaratado hasta el punto de que todo el mundo pudiera disfrutar de ella, sigue existiendo una parte de la población que no tiene la posibilidad de disfrutar y cultivarse.

La exclusión en la era digital debería ser un problema en vías de extinción, pero debido al endurecimiento de las leyes de restricción de copia, no

parece que vaya a desaparecer. Más aún, aumenta paulatinamente. A largo plazo, la excesiva dureza de la legislación sobre derechos de autor tendrá efectos muy negativos en la sociedad, ya que sólo quienes puedan pagar por ella tendrán acceso a la cultura, privando a las clases más desfavorecidas fuera del acceso a grandes clásicos de la humanidad. Esto es precisamente lo que se conoce como exclusión cultural: el proceso por el cual una parte de la población queda fuera de los círculos que permiten el acceso a la cultura, de forma que se mantiene en la ignorancia, ajena a todo lo que hemos aprendido tras siglos de ensayo y error filosófico, científico y social.

5.7.1. Las bibliotecas

En nuestra sociedad se considera algo natural la disponibilidad de un cierto grado de acceso a la cultura, aunque este acceso no existió siempre. Durante siglos, la exclusión cultural fue un mal endémico de nuestras sociedades y eran muy pocos los privilegiados que se libraban de ella. Para combatir este mal, la Ilustración y las revoluciones sociales encontraron como solución el establecimiento de un sistema público de acceso a la cultura que tiene como símbolos los sistemas educativos y las

bibliotecas públicos.

Que la existencia de un sistema educativo universal desempeña un papel crucial en la cultura que adquiere la población es un hecho innegable, aunque sea igualmente irrenunciable el derecho de los padres a elegir qué tipo de educación recibirán sus hijos. Las bibliotecas pasan mucho más inadvertidas, a pesar de encarnar al máximo el espíritu de inclusión social, igualdad y dotación de oportunidades a las clases más pobres, así como el espíritu de las revoluciones sociales que permitieron el nacimiento de las democracias modernas: la posibilidad de adquirir una cultura al alcance de todos, puedan pagarla o no.

Por supuesto, las bibliotecas suponen un problema para la industria del *copyright*. En una biblioteca pública el libro se compra una vez y se lee muchas. Y por eso las bibliotecas, que en los últimos años permitían también el préstamo de música y películas, están actualmente amenazadas de muerte. Lo que se pretende es desmantelar este sistema para que la única opción de acceso a la cultura sea el pago previo por la misma.

Esta batalla se libra en muchos frentes, y no es el menos importante de ellos el de la desinformación. Oímos en

multitud de ocasiones que las bibliotecas no se usan, pero el último informe anual del Instituto Nacional de Estadística sobre el uso de bibliotecas revela un incremento durante el año 2006,[99] algo que no me extraña, ya que siempre que voy a una biblioteca pública veo bastantes personas en ella. Al parecer, la sociedad sí las usa y no son tan superfluas.

Las bibliotecas y las suscripciones digitales

Un problema derivado de la digitalización de la información y del maltrato deliberado que sufren las bibliotecas públicas es el modelo de suscripciones digitales que han adoptado muchas de ellas sin que la comunidad fuese consciente de los problemas que acarrea este tipo de suscripción.

Por citar un caso: las editoriales que gestionan gran parte de la información técnica y científica imponen unas condiciones de cesión de derechos de reproducción bastante abusivas y han apoyado firmemente el cambio de modelo (del envío de las revistas en formato clásico de papel a la suscripción digital a través de la red con acceso a los mismos recursos). Han convertido lo que debía ser un recurso de apoyo a la edición en papel en la columna vertebral,

alegando la necesidad de reducir costes. Y están en su derecho de defender lo que es mejor para ellos, como luego veremos.

Lo que no es apropiado es que multitud de bibliotecas universitarias cambien su suscripción del modelo de recepción de ejemplares en papel a la suscripción digital. Este modelo entraña un peligro real: si la biblioteca deja de recibir los fondos que se utilizan para pagar la suscripción, o si la editorial decide endurecer las condiciones de uso de la misma, podría perderse el acceso a todos los recursos que se han estado pagando durante años de subscripción. Entonces, ¿qué hemos hecho todo este tiempo? Tirar el dinero.

La digitalización de las obras es muchas veces una ventaja. En este mismo caso el acceso electrónico a las publicaciones especializadas es un complemento importante, nunca una alternativa. Y sin embargo no son pocas, de hecho son bastantes, las bibliotecas universitarias que han adoptado este modelo de suscripción: la trampa del *streaming*, que obliga a pagar por los datos indefinidamente bajo la amenaza de quedarse sin acceso a lo que ya se ha pagado.

5.7.2. DRM

DRM es el acrónimo que se utiliza para designar a las medidas anticopia digitales que la industria bautizó con el confuso nombre de gestión de derechos digitales (Digital Rights Management). El DRM no es más que un pequeño código que se inserta en cada archivo digital y te indica lo que *no* puedes hacer con él. El que un archivo no se pueda copiar o se pueda copiar sólo un número limitado de veces, el que no se pueda leer en un dispositivo diferente, el que no se pueda imprimir o el que su texto no se pueda *copiar-pegar* son restricciones que se definen mediante este pequeño trozo de código. El DRM juega un papel esencial en la generación de exclusión cultural.

En realidad, más que gestionar derechos digitales lo que el DRM gestiona son restricciones digitales. Por este motivo, fuera del lenguaje utilizado por la industria, a este código se le da otro nombre que responde a las mismas siglas pero representa mejor su verdadera naturaleza: Digital Restrictions Management (DRM) o gestión de restricciones digitales.

La totalidad de sistemas de DRM se aseguran a través de la ocultación del algoritmo que implementa los

códigos que sirven para gestionar los permisos. Este tipo de estrategia se conoce como "seguridad mediante oscuridad" o *security through obscurity*.[100] Estos métodos de gestión de la información no son en absoluto seguros y la verdadera seguridad no debe nunca recaer en la ocultación de los algoritmos, sino en un buen diseño de los mismos. Por eso no se conoce un sistema de DRM que no haya sucumbido a las legiones de individuos y programadores hábiles que se ponen manos a la obra para conocer el funcionamiento interno de estos sistemas y descubrir cómo evitarlos.

Las motivaciones de estos programadores pueden ser tan variadas como el afán de protagonismo, el simple reto intelectual o la mera reclamación de un derecho básico, el de escoger cómo utilizar los dispositivos o las obras culturales por las que ya se ha pagado. Este último fue el leitmotiv que llevó a Jon Lech Johansen, más conocido en la red como DVD Jon, a desentrañar el funcionamiento del sistema de restricción digital de los DVD. Jon había comprado un DVD que quería ver en su sistema operativo GNU/Linux, pero la restricción en estos discos era tal, que no se podían reproducir en un sistema distinto a Microsoft Windows. Jon Lech Johansen descifró mediante ingeniería

inversa el DRM de estos discos y publicó su trabajo bajo una licencia libre, haciendo posible que el resto del mundo pudiera usar sus DVD de forma libre.

A pesar de estos fracasos, la industria sigue empeñada en introducir estos sistemas de restricciones digitales, en cuyo desarrollo gasta grandes sumas de dinero. Este comportamiento por parte de la industria parece completamente ilógico, y lo es si consideramos la situación atendiendo a la economía de la atención en un ecosistema abundante. Sin embargo, si consideramos que el objetivo último de los sistemas de DRM es eliminar esa abundancia de obras libres para reducir la oferta a una artificialmente escasa, los sistemas de DRM cumplen su función: generar toda la exclusión que puedan, reducir en lo posible el número de copias disponibles para conseguir que aumente el precio de éstas.

En términos de exclusión generada, los DRM son un gran problema. Estos sistemas son cada vez más complejos y difíciles de desbloquear, cada vez requieren más conocimientos técnicos e incluso en ocasiones es necesaria la manipulación física de los circuitos integrados de los dispositivos. Esto hace que, cada vez más, sólo una reducida

élite disponga de las herramientas y los conocimientos necesarios para acceder a la información. Aun cuando se desvelen los esquemas de funcionamiento de la restricción y se publique en Internet para que todo el mundo sepa cómo desbloquear un determinado tipo de contenidos, habrá una parte de la población que no logrará acceder a la información sin pagar los precios cada vez más exigentes que imponen los oligopolios culturales que basan su negocio en las restricción de copia. El que no esté de acuerdo, que se pregunte a sí mismo a cuántas personas conoce que no saben cómo hacer una copia de seguridad de un DVD original (DVD9) en un DVD virgen convencional (DVD5); yo conozco bastantes y parece que no soy el único, pues según un estudio publicado en *The New York Times*, sólo el 1,5 % de los usuarios tienen instalado software para copiar DVD, y se estima que dos terceras partes de ese porcentaje, ya pequeño de por sí, no lo usan nunca.[101] Pues bien, si aún necesitaban una definición de exclusión, eso es exclusión: los sistemas de DRM *son* exclusión.

5.7.3. La compensación por copia privada o canon

Compensación equitativa por copia privada es el

nombre de un impuesto indirecto cuyo valor nominal es establecido por el Estado y cuyo destinatario no es el erario, sino un conjunto de empresas privadas. Este gravamen se aplica a multitud de dispositivos a los que se considera «equipos, aparatos y materiales idóneos para realizar dicha reproducción» de material protegido por derechos de autor.[102] Actualmente esta definición es tan vaga, que hasta un reloj con memoria USB se incluye en esa categoría, aunque probablemente nadie decida va a usar su reloj de pulsera como reproductor ni almacén de audio, vídeo o libros. Eso hace que todo tipo de dispositivos sean gravados con este impuesto, independientemente de su uso final. Su carácter arbitrario y omnipresente propició que en la calle esta compensación por copia privada recibiera un nombre mucho más directo y menos cariñoso: *canon*.

Su carácter necesario en toda compra y su naturaleza *ab initio* y anterior a la consumación de toda copia privada hacen de este canon un impuesto terriblemente injusto y odiado por la sociedad. Además, las más que dudosas hipótesis del lucro cesante en que se asienta han sido negadas anteriormente, afirmándose que el lucro cesante generado por la compartición de archivos era

estadísticamente indistinguible de cero.[103] Otros autores, como David Blackburn, comentan incluso que la compartición de archivos en la redes de pares tiene efectos estadísticamente positivos en las ventas de la mayoría de los artistas, y sólo una pequeña minoría ve reducidas sus ventas.[104]

Por todo lo anterior, el pago de un tributo de dudosa necesidad y pertinencia han hecho que este pago se vea popularmente como una tasa impuesta por unos pocos al conjunto de la sociedad y ha pasado a ser contemplado como un impuesto revolucionario que hay que pagar a una serie de empresas con oscuros intereses y nula transparencia en sus cuentas.

La lógica económica del canon es la de cobrar múltiples veces por un mismo servicio. Las empresas del sector cultural pretenden cobrar por vender la copia, que eventualmente incluirá medidas anticopia, pero también nos cobran un canon compensatorio por todos y cada uno de los dispositivos que adquirimos; no sólo a nosotros, sino a todo el mundo.

Como consecuencia de esta inflación del precio, el canon repercute al alza en el precio de los dispositivos que

nos permiten acceder a las obras culturales y es, por tanto, una medida excluyente. Además, con el aumento de la disponibilidad de cámaras de fotografía y vídeo digital, cada vez utilizamos más discos para almacenar nuestro propio material, lo que hace del canon un impuesto injusto. Para rematar los puntos negativos de este impuesto, tenemos que, para salvar una industria, la del *copyright*, se encarece el producto de otra industria, los fabricantes de dispositivos de almacenamiento de todo tipo, que ven cada vez más que la solución más barata es importar soportes vírgenes del extranjero. Esto destruye lentamente el tejido industrial interno: en España, tras la instauración del canon digital, no ha sobrevivido una sola de las fábricas de CD que había.[105]

No me extenderé más sobre el tema del canon, un tema muy controvertido. Existen multitud de reflexiones sobre este asunto de personas que saben mucho más que yo sobre él.[106,107] En general, no resulta difícil encontrar personas que, aun defendiendo las mismas ideas, realicen aproximaciones diferentes de este asunto. Sin embargo, casi todos están en el mismo bando y, aunque difieran en la forma, sus motivos concurren y los unen: quieren la libertad de copia porque es un derecho natural que nos quieren

arrebatar.

La incompatibilidad DRM-canon

Para hablar de la incompatibilidad DRM-canon tenemos que volver al principio de este asunto: las diferencias de enfoque en el derecho continental y el derecho norteamericano en cuanto a los derechos de autor y los derechos de reproducción. Estos dos sistemas mantienen dos visiones muy diferentes. El DRM intenta impedir la realización de copias privadas de una obra, algo que no está permitido en varios países, mientras el canon intenta compensar equitativamente a los autores por las copias realizadas.

El problema es que la mayoría de obras que se venden actualmente incluyen medidas anticopia (todas las películas en DVD y gran parte de la música), mientras el canon sirve para compensar al autor por las copias privadas que se hacen de su obra y que las medidas anticopia ya mencionadas no permiten realizar. Sucede que, a pesar de la inclusión de estas medidas anticopia, se sigue reclamando la compensación por copia privada.

Lo terrible de esta situación es que la inclusión de

estas medidas anticopia debería eliminar todo derecho de estos editores y artistas a percibir compensación económica por copia privada pero, lejos de eso, el gobierno mira hacia otro lado e incluso legisla a su favor, extendiendo el canon compensatorio y aumentando su cuantía en la última reforma de la Ley de Propiedad Intelectual.[108]

El canon en las bibliotecas

Recientemente se ha legislado en España para que los autores reciban una compensación económica cada vez que se preste un libro en una biblioteca pública. Esta compensación ha sido «impuesta desde Europa», en lo que es otro amargo ejemplo de cómo mediante el Consenso de Washington se consigue que a nuestros políticos no se les culpe por multitud de decisiones que atentan contra nuestros derechos.[109] Este canon se impuso ignorando campañas que, desde el ámbito universitario, llevaban años avisando y luchando en contra del mismo. Se llegó a recoger más de un millón de firmas contra este canon por préstamo bibliotecario.[110]

La inclusión del canon por préstamo bibliotecario se enmarca en la misma estrategia que el canon por copia

privada en contenidos audiovisuales, la de cobrar infinitas veces por un único producto, y se justifica atendiendo a la misma falacia del lucro cesante: asumir que todo aquel que toma un libro de una biblioteca lo compraría si no pudiera sacarlo de la biblioteca y que, de ese modo, un libro prestado es un libro que se deja de vender. De esta forma, el editor cobra el libro y posteriormente vuelve a cobrar por todas y cada una de las personas que lo toman prestado. Un negocio redondo y otra mentira editorial que los partidos políticos que nos gobiernan han amparado y legalizado.

Después de haber descrito las bibliotecas como una de las mayores victorias, y sin duda una de las más valoradas, de las revoluciones sociales y las democracias modernas, huelga decir que el canon por préstamo bibliotecario (también recogido por entidades privadas carentes de toda transparencia) es una mala noticia. La progresiva conversión de las bibliotecas en librerías es una medida nefasta que genera exclusión cultural y que atenta contra uno de los derechos fundamentales: el libre acceso a la cultura.

De forma colateral también afecta a la libertad de expresión y de opinión, pues supone una traba adicional en

el libre flujo de ideas y de conocimiento y, lo que es más crítico, al desarrollo de un criterio propio por parte de cada persona. En este sentido, el que las bibliotecas se transformen legalmente en librerías es un cambio tan desolador como lo ha sido observar que la reforma se ha implantado de espaldas a la sociedad española, que ha guardado el silencio que guardan quienes desconocen completamente tanto las medidas políticas que se están aprobando como las probables consecuencias de las mismas a medio y largo plazo.

5.7.4. El sistema de streaming *global: la* jukebox

Pasar de un modelo de venta a un modelo de suscripción es la mayor de las ambiciones de la industria del *copyright*; su sueño dorado. Este modelo de suscripción es también conocido como modelo de la *jukebox*[34] o la *jukebox global*, en alusión a la clásica máquina de música. En Internet y en la actualidad el modelo de *jukebox* está encarnado en los sistemas de *streaming*, en los que se da el tránsito de datos pero éstos no se almacenan, sino que se reproducen en tiempo real y luego se tiran a la basura. A menudo el almacenamiento está bloqueado empleando la gestión de restricciones digitales.

En el modelo convencional, la opción por defecto sería siempre guardar los datos, sean datos de audio (como una canción, un programa de radio o un podcast) o de vídeo (como una película, un pequeño vídeo de youtube o una noticia informativa). Una vez decidamos que no queremos volver a verlos, tendríamos libertad para eliminarlos, pero si decidimos volver a verlos podremos hacerlo sin depender del nodo que nos sirve los datos.

En el modelo de la *jukebox*, cada vez que queremos oír algo tenemos que acceder a ello de forma remota, hay un servidor que nos transfiere los datos en cada momento y que controla absolutamente la transacción. Si decide eliminar el fichero, ya no tendremos acceso al mismo. ¿Es una ventaja tener que de nuevo una información para volver a acceder a ella? Visto así no lo parece.

La industria del *copyright* se empeña en instalar sistemas de este tipo, ya que la dependencia que crean respecto del proveedor de los contenidos es total, y es precisamente esta situación de superioridad total la que le permitirá dar un paso definitivo hacia la culminación de su estrategia de escasez artificial: el pago por suscripción y la imposición de las condiciones de acceso a los datos remotos.

Con el aumento de las capacidades de transmisión de datos a través de Internet en los últimos años se ha potenciado la emisión de datos en *streaming*, amparándose en la idea de que no necesitas almacenar esa canción o vídeo ya que apenas se tarda en volver a acceder a la red y acceder a los contenidos de nuevo. Se oye una canción o se ve una película, pero ésta no se almacena permanentemente en nuestro sistema. El establecimiento de este sistema es uno de los grandes sueños dorados de la industria del copyright: si se alcanzara un punto en que nadie tuviera un almacén de datos local, para acceder a una determinada información habría que aceptar las condiciones impuestas por la industria. Por lejano que pueda parecer, el sistema de «la *jukebox* global» va ganando terreno poco a poco, aunque de forma inadvertida. Un ejemplo fue el anuncio, aplaudido desde muchos sectores, de *Last.fm* de que se iba a permitir oír la canción que se quisiera un número limitado de veces;[111] estos archivos tienen DRM, pero seguramente habrá quien acepte este sistema y deje de tener almacenada su propia copia no restringida del fichero.

Este modelo, que puede parecerle lejano a muchas personas, está más asentado de lo que parece y se consolida

con cada reforma legal que se realiza en este ámbito. El problema es que, una vez que se cancela la suscripción, se pierde por completo el acceso a los ficheros, incluso a los que se tengan almacenados localmente. Este modelo es el que utilizan diversos sistemas de alquiler de música online como Napster y la gran mayoría de editoriales académicas a las que las universidades se han suscrito atraídas por una reducción de costes sin pensar en la dependencia que generan del proveedor.

El modelo de suscripción universal avanza también en otras ramas de la industria del *copyright*, como la industria editorial, con el canon de préstamo bibliotecario.[112] Si un buen día el editor decide no renovar el contrato, o la universidad ve reducido su presupuesto para la biblioteca y no puede pagar la suscripción, se perderá el acceso a todas las publicaciones, incluso a aquellas que se han pagado obedientemente durante años.

¿Quién quiere *streaming?*

Aún queda una cuestión pendiente relacionada con la *jukebox* global y el *streaming* continuo de datos. ¿Quién quiere *streaming* continuo? ¿Quién les ha dicho a los

vendedores que no nos gusta almacenar nuestros contenidos localmente? ¿Acaso creen que las redes p2p sirven para usar y tirar lo que circula por ellas o que no nos gusta tener nuestro reproductor de mp3 cargado de música hasta los topes? ¿Alguien les dijo que no nos gusta leer nuestras revistas o escuchar nuestra música cuando no tenemos acceso a la red?

La realidad es que no queremos *streaming*. El *streaming* es abusivo por el tipo de relación proveedor-receptor que genera. Nos deja indefensos antes los deseos y las exigencias de un nodo de la red que no es como nosotros, ya que controla lo que podemos ver. Una red así construida no es distribuida, sino descentralizada, es un paso atrás en el sistema que Internet hace posible.

No podemos negar que la industria se movió muy rápido en esta dirección. Sabedora de que la revolución tecnológica haría tambalearse su negocio, se adelantó algunos años a las redes de pares cuando en los primeros años noventa comenzó a presionar a los gobiernos para que extendieran y endurecieran la legislación sobre restricción de copia, que hasta ese momento había sufrido reformas periódicas pero a largo plazo, algo que, por muy típico que

pueda sonar, en los últimos años se ha acelerado vertiginosamente.

Sin embargo, la realidad actual es un jarro de agua fría para este modelo soñado: ahora podemos obtener gratis todo lo que la industria no ceja en su empeño de ofrecer vía *streaming* manteniendo un control total. Pero no debemos descartar que un cambio en la red o un rediseño legal actúen como fuerza coercitiva y modifiquen el estado actual de las cosas. Las leyes -endurecimiento de penas por infracción de derechos de autor, compensaciones por copia privada- han asegurado que, al menos a corto plazo, la industria pueda no sólo subsistir, sino crecer a un ritmo acelerado gracias al pago obligado de impuestos que van a parar directamente a sus arcas. En nuestras manos está evitar que este modelo continúe su expansión, algo que sería muy negativo por los altísimos niveles de exclusión que generaría.

5.7.5. El cercamiento digital

Se conoce por "cercamiento" a la medida promovida por los terratenientes en el Reino Unido (posteriormente, extendida al resto de Europa, hasta llegar a Andalucía y Cataluña) que a partir del siglo XVII abogaban por que se

vallaran los campos de cultivo que hasta entonces no habían pertenecido expresamente a nadie y habían sido explotados de forma comunitaria. La excusa era que si los campos estaban en manos privadas, iban a producir más comida para todos. «La gestión privada salvaría vidas.» Al estar el campo en manos privadas se dificultaba el acceso a algo que, hasta entonces, había sido de uso común. Posteriormente se demostró que los campos no producían más, pero se favoreció la concentración de tierras, la aparición de latifundistas y terratenientes. Durante el siglo XVIII hubo muchas tensiones sociales por culpa de esta cuestión.

Ahora estamos viviendo un nuevo cercamiento de distinta naturaleza: el cercamiento digital. Un nuevo intento de poner vallas al campo y convertir en propiedad de unos pocos lo que antes era propiedad de todos o, más formalmente aún, ni siquiera era propiedad de nadie porque hay cosas que no se pueden poseer: nos referimos a las ideas y al uso y restricción que de ellas hacen las nuevas leyes de propiedad intelectual. Parece que no hemos avanzado nada en casi cuatrocientos años, ya que, por ejemplo, Monsanto pretende convencer al mundo de que la concesión de un monopolio sobre el arroz transgénico salvará vidas, cuando

es precisamente la conversión al monocultivo del arroz de Monsanto y sus enormes campos de cultivo lo que hace que en numerosas zonas de Asia haya malnutrición (pues se ha abandonado por el arroz el cultivo de otro tipo de vegetales que les aportaban vitaminas). Monsanto prohíbe que otras personas planten arroz modificado aduciendo que posee la propiedad intelectual sobre la modificación.

El cercamiento digital avanza con cada nuevo intento de ampliar la cobertura de patentes al software y la medicina, con cada nuevo intento de fortalecer la restricción de copia y de alargar la vida de los monopolios de explotación exclusivos de obras culturales y científicas y sus consecuencias se traducen en una restricción de lo que podemos hacer con las cosas que pagamos o con cosas como la reducción del derecho a cita en la reforma de la Ley de propiedad intelectual introducida en 2006. Cercar, bloquear, limitar, sin que importe que los derechos de réplica, la libertad de expresión e información se pierdan por el camino. Vallas y más vallas, y sobre algo que hace medio siglo nadie se habría cuestionado. ¿Compartir es malo? ¿Copiar una canción es como robar un coche? ¿Acaso mi copia desactiva la canción original?

Las leyes de propiedad intelectual no son un brindis al cielo para apoyar a unos cuantos artistas y a un sector de la industria. Las LPIs del mundo son parte de un todo más grande, y el que no quiera entenderlo que no lo entienda, pero Quizá mañana sea demasiado tarde para revocar las leyes restrictivas que se introduciendo.

5.7.6. El endurecimiento de las leyes de restricción de copia en el contexto del cercamiento digital

Ya hemos mencionado que en todo el mundo se está produciendo un endurecimiento excesivo de las leyes de propiedad intelectual como parte de un proceso de privatización de un espacio (el de las ideas y las creaciones) que en el pasado pertenecía a todos (ni siquiera existía el concepto de que pudiera pertenecer a alguien), limitando el derecho de acceso a los demás. Esto proceso es lo que conocemos como cercamiento digital y en los últimos años interviene, junto con otras medidas, en el desarrollo de la sociedad de control. La batalla por imponer la restricción de copia se enmarca, pues, dentro de un proceso mucho más ambicioso.

El mecanismo por el que este tipo de leyes se va

endureciendo en todo el mundo está controlado por los intereses económicos de la mayor potencia del mundo, Estados Unidos, y su poderosa industria del entretenimiento. La economía de Estados Unidos es básicamente importadora, si no tenemos en cuenta las exportaciones tecnológicas -que casi en su totalidad se producen a Asia- ni las militares. Pero esta economía tiene en los productos de ocio y culturales un auténtico filón de oro para sus exportaciones, y este sector llega a representar en torno al 10 % de su PIB. Ante esta evidencia, el gobierno de Estados Unidos promueve por todo el mundo un endurecimiento de las leyes de restricción de copia para que en otros países no resulte fácil copiar legalmente estos productos y en todas partes las personas estén obligadas a comprárselos a su industria, que es la que sale beneficiada con todo este asunto.

El sistema es curioso y comprende el empleo de técnicas de persuasión absolutamente mafiosas. Como ejemplo, Estados Unidos se permite bloquear el ingreso de países en las instituciones internacionales como la OMC -y no compete aquí analizar si esta institución es positiva o negativa-, pidiendo como moneda de cambio el

endurecimiento previo de estas leyes. Así sucedió con China, y así sucede con Rusia, que aún espera poder entrar en el club de la OMC. Los grupos de presión empresariales estadounidenses presionan a estos gobiernos imponiendo medidas aún más restrictivas que las existentes en Estados Unidos para poder exigir a continuación un endurecimiento de las leyes en su propio país con la excusa de «armonizar la legislación» con la que ya existen en el ámbito internacional. Por supuesto, y para que ningún ciudadano pueda quejarse a sus gobiernos, todo ello se hace a través de un intermediario: la World Intellectual Property Organization, WIPO. Así los gobiernos parecen estar acatando directivas externas.

Sin duda esto ha funcionado enormemente bien en el caso de los países pobres y, aunque también ha tenido éxito, éste ha sido menor en los países ricos. Sin embargo, últimamente los países ricos que mejor habían aguantado estos envites pro-*copyright* están cediendo e imponiendo niveles tan restrictivos como el estadounidense (a veces más, si finalmente se aprueba en Europa el modelo de desconexión y censura por usar sistemas p2p). Tenemos el ejemplo de Suiza, que aprobó «su DMCA» en octubre de

2007, y tenemos también el caso de Canadá, que prepara una ley de propiedad intelectual tan dura como la DMCA estadounidense[113] bajo la presión directa de los senadores estadounidenses.[114]

Por supuesto, todas estas leyes incluyen artículos que explícitamente prohíben la eliminación y burla de medidas digitales de restricción de derechos (DRM), ya que así se exige desde la WIPO, en otro claro ejemplo de cómo los ciudadanos están a dos grados de separación del poder, pues sus gobiernos están sometidos a organizaciones que nadie elige democráticamente, una política extendida mediante lo que conocemos como Consenso de Washington.

5.8. La exclusión como imposición de la brecha digital

El concepto de brecha digital es uno de los pocos conceptos relacionados con Internet que a menudo llegan hasta el mundo real y ocupan titulares en los medios de comunicación. Aún reconociendo esto, el concepto de brecha digital que suelen manejar estos medios difiere bastante de lo que en realidad es la brecha digital, entendida como algo que crea desigualdad entre los individuos.

La brecha digital, tal y como se menciona habitualmente, tiene que ver con el acceso a la red. La verdad es que la brecha digital y el acceso a la red no son la misma cosa, de modo que asociar ambos conceptos es erróneo. Quizá en la actualidad podemos separar a las personas en función de si tienen acceso o no a la red, pero pronto, aún antes en los países ricos, todo el mundo tendrá acceso móvil a la red. En esas circunstancias, ¿desaparecería la brecha digital? ¿Cómo debemos definir la brecha digital?

No parece probable que la brecha digital desaparezca el día en que toda la población tenga acceso a la red. En un mundo siempre conectado donde todas las personas tengan acceso a la red, la verdadera brecha digital no es el acceso a la red, sino poseer la educación suficiente para saber usarla. El reto en la red es saber emplear las herramientas que te pone en la mano para no perder el rumbo. La exclusión, que define la cultura y el grado de ilustración que podrá adquirir una persona, juega en esta *nueva* brecha digital un papel importante. La brecha digital no es algo nuevo, sino que es la traslación a la sociedad digital de la más antigua de las desigualdades sociales: la del acceso a la educación.

La generación deliberada de exclusión mediante la creación de leyes que van endureciendo el acceso a la cultura (eliminación de bibliotecas públicas, restricción de copia) se convierte entonces en un mecanismo para mantener a la población bajo control limitando su propio criterio y su capacidad de uso de la red.

5.9. Software libre, *copyleft*, ética

Los movimientos de *copyleft* y de software libre son una de las mayores sorpresas que la era digital nos ha deparado. Representan unos de los movimientos sociales y filosóficos más interesantes de la actualidad y constituyen en sí mismos toda una demostración de poder.

El software libre es la demostración de que los principios de la ciencia, aplicados allá donde sea posible hacerlo, generan un mayor progreso y lo hacen más rápidamente. El software libre demuestra que no sólo no es necesario reservarse todos los derechos de «propiedad intelectual» para tener éxito, sino que el éxito puede deberse precisamente al hecho de que no lo hagamos en absoluto. El movimiento *copyleft* era al principio indisoluble del movimiento del software libre, pero poco a poco y

debido a la aplicación de las libertades propugnadas por el movimiento de software libre a todo tipo de creaciones, en la actualidad se le identifica como algo diferente; de hecho, ahora el término *copyleft* se utiliza para muchas cosas que formalmente no son *copyleft*, como luego veremos.

El término *copyleft* es una burla del término anglosajón *copyright*. Aunque el concepto al que se refiere fue ideado por Richard Stallman, principal ideólogo y filósofo detrás del movimiento del software libre, quien también popularizó mundialmente el mismo, el término *copyleft* no lo acuñó él originalmente, sino que fue Don Hopkins quien lo utilizó por primera vez alrededor de 1984 o 1985. Don Hopkins tuvo la ocurrencia de incluir en una carta el siguiente proverbio: «*Copyleft*: quedan revocados todos los derechos». Según nos cuenta Richard Stallman en su libro *Software libre para una sociedad libre*.[115]

5.9.1. Los orígenes del movimiento del software libre

Si hay algo que llama poderosamente la atención respecto al movimiento de software libre es que es un movimiento ético. El leitmotiv de los padres del movimiento del software libre no es obtener un mejor sistema de

desarrollo de software, aunque fueran conscientes de que el planteamiento que ellos tenían era en sí mismo ese sistema optimizado y aunque el tiempo les haya dado la razón.

Copiar, compartir, colaborar, todas ellas son acciones naturales en los seres humanos. Es así como el ser humano ha avanzado hasta la actualidad, especialmente desde que se desarrolló un método científico que permitió optimizar el modo en que se comparte, copia y modifica la información y los conocimientos para obtener nuevos conocimientos a partir de ahí. Cuando se diseñó la red, este diseño obedeció al más escrupuloso método científico. Se desarrolló en un laboratorio, pero los principios que la regían fueron puestos a disposición de todos, bajo dominio público, para que todos pudieran trabajar sobre la idea, modificarla, mejorarla y depurarla. Otro tanto había sucedido unas décadas antes, en los albores de la informática y la electrónica.

En aquella época Richard Stallman trabajaba como investigador en el departamento de Inteligencia Artificial del Instituto de Tecnología de Massachussets (MIT).[116] En ese laboratorio trabajaba un grupo de personas acostumbradas a desarrollar código colaborativamente hasta que, a

comienzos de la década de los ochenta, el grupo se desintegró y sus miembros fueron recolocándose en el sector privado dentro de la incipiente industria del software.

Esta industria desarrollaba (y aún lo hace) software, pero no sigue los principios de la ciencia de poner a disposición pública los avances obtenidos. De este modo se crea una dependencia respecto del proveedor de software, que es el único que conoce cómo funciona un programa y es el único que dispone de las herramientas para modificarlo y mejorarlo: al usar software no libre se es cautivo de los caprichos del fabricante. Estas empresas se anunciaban como empresas de «valor añadido», pero lo único que añaden es lo que a esas empresas le habría gustado que hiciésemos: adoptar la comodidad de pagar por un software con restricciones antes que la libertad de desarrollar un software libre con el que trabajar sin limitaciones. En realidad, estas empresas vendían un software con restricciones de uso, por lo que Stallman pensó que deberíamos hablar de empresas y productos de «libertad sustraída» o «privativos».[117] Dos décadas después de aquellos comienzos, el movimiento del software libre, en palabras del

propio Richard Stallman, «ha ganado batallas que él no preveía ganar».[118]

Definición de Software Libre. La licencia GPL.

Para que un software sea libre es necesario que cumpla unos requisitos mínimos. Estos requisitos son lo que se conoce como «las cuatro libertades del software libre» y juntos constituyen la definición del "software libre". Las cuatro libertades incluyen la libertad de copia, modificación, mejora y redistribución de un programa sin restringir estas libertades.[119]

Estas cuatro características del software libre quedaron plasmadas en un texto legal de licencia elaborado por la Fundación del Software Libre (FSF, Free Software Foundation): la Licencia Pública General o GPL (General Public License). Esta licencia es, con diferencia, la más empleada entre las disponibles para los miles de proyectos de software libre existentes en la actualidad, si bien no es la única. En 2007 se ha lanzado la tercera versión de esta licencia GPL, que permite adaptarla a la legalidad más actual, si bien las cuatro libertades básicas del software libre no se han modificado, ya que son una definición conceptual.

Free Software Foundation, GNU

El movimiento del software libre iniciado por Richard Stallman es un movimiento de respuesta a esta nueva industria del software que se materializó en la Free Software Foundation (FSF) o Fundación Software Libre. Esta fundación, que carece de ánimo de lucro, se centraría en dar a conocer la idea de software libre, así como en promover y desarrollar este software.

En un mundo en el que aún no existía *Windows*, la mayoría de las computadoras funcionaban con sistemas tipo UNIX, el sistema desarrollado en la Universidad de Berkeley. UNIX no era libre y como la mayoría del software existente era para este sistema, el primer objetivo de la FSF fue el desarrollo de un conjunto completo de software libre completamente compatible con Unix. Este conjunto de software conformaría el sistema operativo GNU (GNU is Not Unix, acrónimo recurrente), de forma que el principal objetivo de la FSF fue el desarrollo de GNU, un sistema operativo completamente libre y totalmente compatible con el sistema dominante en aquella época: UNIX.

5.9.2. FDL, Creative Commons, la devaluación del copyleft *y el movimiento devolucionista*

La licencia pública general (GPL) sirve para definir el software libre en el contexto de un contrato de usuario. De este modo se garantiza que la persona que adquiere el software realmente lo adquiere para trabajar con él libremente, más allá de adquirir el derecho a utilizar temporal y limitadamente el mismo. La FSF descubrió posteriormente que no existía documentación libre sobre software libre. Todos los libros especializados estaban publicados bajo condiciones de restricción de copia. Un nuevo objetivo de la FSF fue la creación de un repositorio de obras libres que permitieran aprender a utilizar y desarrollar software libre.

Con ese propósito se adaptó la licencia pública general al desarrollo de textos, obteniéndose la que se conoce como Licencia de Documentación Libre o FDL (Free Document License). Esta licencia debía preservar la libertad de los textos del mismo modo que la GPL preserva la libertad del software.

Una década después, Lawrence Lessig crearía Creative Commons y su sistema de licencias *copyleft*

graduales, que permiten controlar los permisos que se ceden de una determinada obra.[120] Estas licencias no son sólo aplicables a obras escritas, y recibieron de los blogs y de la blogosfera la aceptación y el impulso necesarios para crecer y darse a conocer, representando el conjunto de licencias más utilizado en este tipo de publicaciones.

Las diferencias conceptuales entre las licencia de documentación libre y las licencias Creative Commons son enormes, aunque en la práctica algunas de ellas sean compatibles y otras tengan efectos similares. Mientras las licencias libres de la FSF, como la licencia de documentación libre, rechazan la existencia de algo similar a la propiedad intelectual («todos los derechos rechazados») como vía para la creación de un verdadero pozo de conocimiento común que beneficie a toda la sociedad, las licencias Creative Commons persiguen *otorgar al autor más control sobre su obra*. De este modo, mientras unas aspiran a la creación de un procomún social, otras pretenden devolver a los autores las libertades que los editores les habían arrebatado; mientras unas rechazan el actual sistema de propiedad intelectual, otras lo aceptan implícitamente. Sólo tangencialmente ambas visiones mantienen un punto de contacto: cuando

muchos autores que deciden publicar mediante Creative Commons escogen dar libertad de uso a sus obras, puede producirse un procomún similar al que permiten las licencias verdaderamente libres. Sin embargo, esta situación no es el fin último del sistema de licencias ideado por Lessig, sino una consecuencia lateral beneficiosa.

Aunque permiten el acceso gratuito a muchas obras, el hecho de que muchas modalidades de licencia Creative Commons no sean verdaderamente libres (entre ellas, las que no permiten el uso comercial de las obras) genera rechazo entre los más firmes partidarios de la cultura libre. Entre las oposiciones más llamativas tenemos la postura de los *devolucionistas*. Por "devolución" entenderemos el acto de ceder voluntariamente al dominio público todos los derechos sobre una obra, de forma que ésta pueda ser modificada, reutilizada y publicada a voluntad y sin obligar a que las obras derivadas sean también libres ni formen parte del dominio público.[121]

Mientras los partidarios de Creative Commons abogan por este tipo de licencias como medio para evitar la apropiación de las obras por parte de la industria de la cultura privativa, los devolucionistas opinan que aceptar las

licencias Creative Commons es aceptar las tesis de la propiedad intelectual que propone este sistema excluyente. Al otorgar «más control a los autores» se configura como un sistema que, lejos de favorecer la progresiva abolición del sistema de propiedad intelectual actual por otro más respetuoso y menos excluyente, la ralentiza, pues se defiende el derecho a compartir las obras desde la fortaleza de la propiedad («Esto es mío, y no de la industria, por tanto se compartirá como yo diga») y no desde el ideal de la cultura libre («Nadie puede reclamar propiedad sobre una obra intelectual, la autoría no será negada pero no es ético utilizar la autoría para limitar lo que los demás pueden hacer con nuestra obra»).[122]

El principal argumento de los devolucionistas en contra de los partidarios del *copyleft* promovido por Creative Commons es que estos últimos amparan su movimiento en una pregunta: «¿No tiene derecho la gente a controlar cómo se usa su creatividad?». Esta pregunta es una pregunta trampa para los devolucionistas, que argumentan que el control sobre el uso de las ideas propias realmente constituye un control sobre las ideas de otras personas, algo inadmisible que se suele emplear para dificultar más las

vidas y la expresión de las ideas de los demás.

En el punto medio de ambas visiones se encontraría la propuesta de la Free Software Foundation: la licencia de documentación libre. Mientras ideológicamente defiende lo mismo que defienden los devolucionistas, se blinda legalmente contra la apropiación de las obras mediante la exigencia de mantener las mismas libertades originales en toda obra derivada. Y para ello no recurre a la devaluación del término *copyleft* mediante su aplicación a licencias no libres como son la mayoría de licencias Creative Commons. Parece claro, pues, que a la espera de un momento legal más favorable para la cultura libre, el uso de licencias libres y fuertes es la mejor manera de crear cultura libre y asegurarse de que ésta no sea objeto de abusos ni apropiaciones indebidas por parte de nadie.

5.9.3. La migración a la web y el problema del software libre

El software libre ha conseguido poco a poco, y no sin problemas, plantar cara en igualdad de condiciones al software privativo ahí donde éste tenía su principal negocio: las aplicaciones de escritorio. El software libre ha cubierto prácticamente todas las necesidades de los usuarios y les

ofrece la opción de trabajar sin renunciar a la libertad de elección de proveedor en un futuro, al emplear un software que puede ser mejorado por cualquiera (incluso por los propios usuarios si poseen las habilidades necesarias).

Aunque es una batalla que aún hay que terminar de ganar, el software libre ha impuesto su modelo y dispone de las armas adecuadas (ingentes cantidades de programadores que trabajan en un modelo de desarrollo optimizado) para imponer el modelo de libertad frente al modelo restrictivo de la industria del software privativo.

Es precisamente por esto por lo que la industria promueve un nuevo giro: la migración desde el modelo del software en el escritorio al software en la web; un cambio de escenario tal, que el software libre vuelve a estar en desventaja. En los últimos tiempos existe una gran tendencia a trasladar servicios de escritorio a la red. Ofimática, agenda, gestión de fotos, de marcadores, notas y listas de tareas, todo puede realizarse en la red. Y ello se debe a que en este entorno las compañías pretenden recuperar el control sobre el código de las aplicaciones y, lo que es aún más interesante y preocupante, sobre los propios datos de las personas que utilizan sus servicios.

El principal problema es que la mayoría de las aplicaciones web son aplicaciones falsamente libres, desarrolladas y gestionadas con software libre como PHP y MySQL, pero cuyo código ejecutable no está disponible para el libre uso, estudio, redistribución y modificación, ya que jamás llega a salir de los servidores web de la compañía que ofrece el servicio. La retórica de la disponibilidad ubicua de los datos y el hecho de que son aplicaciones desarrolladas con herramientas libres (sin llegar a ser aplicaciones libres) hacen que incluso parte de la comunidad del software libre perciba las aplicaciones web no libres como alternativas válidas a aplicaciones de escritorio clásicas, lo cual resulta especialmente llamativo y peligroso. El caso más visible de este tipo de situación lo ofrece el servicio de correo web de Google. Desarrollado con una calidad y una elegancia notables, Gmail revolucionó el webmail a mediados de 2004 gracias a su enorme capacidad de almacenamiento y su cuidada interfaz. El hecho de que fuera anunciado el 1 de abril contribuyó a que muchos, evidentemente, no se pudieran creer lo que estaban viendo.[123] Sin competidor real en cuanto a servicios web, Gmail es para muchos usuarios una buena alternativa para mantener sincronizados sus datos cuando utilizan más de una computadora, algo muy

frecuente en la actualidad, sobre todo entre los usuarios más habituales.

Esta promesa la realizan numerosos servicios web que, pese a sus buenas cualidades, no ofrecen una libertad total, que vendría encarnada en la disponibilidad de un software que pudieras instalar en un servidor propio para ejecutar la aplicación independientemente del proveedor. Estos servicios basan su negocio en la generación de escasez, que obliga a todo el mundo a acceder a su web para realizar aquello que quieren realizar: comunicarse, acceder a la información, organizar sus tareas.

El problema de migrar las aplicaciones a la web reside principalmente en tres puntos: se crean problemas de privacidad (algo que ya hemos mencionado) que hay que evaluar debidamente para saber cuándo se aceptan, al usar el servicio otorgamos al proveedor enormes cantidades de información personal para uso comercial cuyo valor es altísimo, y se crean relaciones de dependencia respecto del proveedor.

El negocio de las bases de datos

En la sociedad digital han surgido varios retos para

quienes luchamos por evitar que se emplee la tecnología para recortar las libertades en lugar de para garantizarlas y hacer nuestras vidas más fáciles.

La primera de las luchas tiene que ver con el software libre, y va por buen camino; queda mucho por hacer, pero el software libre se va imponiendo cada vez en más ámbitos. La segunda es la lucha por la apertura del sistema de propiedad intelectual para hacerlo más permisivo y libre. Esta lucha está en su momento álgido: si bien es probable que acabe en triunfo, los grupos de presión partidarios de endurecer estas leyes y fortalecer este modelo excluyente son cada vez más poderosos y están consiguiendo reformas legales contrarias al interés general que hacen que el resultado de esta lucha sea incierto.

La tercera lucha es la lucha por la propiedad de las bases de datos y aún no ha trascendido. Y no lo ha hecho porque aún no hemos llegado a entender el verdadero alcance del asunto. Las bases de datos valen mucho dinero, y las bases de datos con información personal sensible, como la formada por todo nuestro correo electrónico, valen aún más. Es el elevado valor de las bases de datos con información personal lo que hace que muchas compañías

(cada vez más) ofrezcan servicios *online* de forma gratuita. El precio a pagar, nos demos cuenta o no, es altísimo y lo pagamos con creces permitiendo el acceso y el uso de nuestra información personal con fines comerciales.

La historia del capitalismo indica que toda nueva revolución comercial se ha cimentado convirtiendo en productos industriales producidos y comercializados en serie y de forma masiva objetos que hasta ese momento eran fabricados de forma artesanal. Así sucedió con la revolución textil en Flandes y con la invención de los transportes masivos de pasajeros (sobre todo el ferrocarril) en la Inglaterra del siglo XIX. Henry Ford convirtió, a su vez, el transporte individual en producto industrial fabricado en serie y, más tarde, la industria de los electrodomésticos nos creó la necesidad de toda clase de pequeños aparatos que hacían las tareas que anteriormente se hacían a mano. Por último, la industria del entretenimiento hizo de nuestro tiempo libre un objeto de negocio. Tal como están las cosas, la próxima revolución comercial no podría más que convertir en objeto de mercadeo lo único que aún no ha sido invadido: nuestra vida privada. Usar la información sobre nuestra vida privada para adaptar los productos que se nos

ofrecen, los anuncios que se nos muestran y las tarifas de los seguros que contratamos (un ámbito en el cual la biometría y la genética jugarán también su rol).

Quizá nadie sabe aún cómo rentabilizar toda esa información. Parece que a día de hoy sólo Google con su Google AdSense y Facebook con su Facebook Flyers poseen herramientas capaces de adaptar la publicidad que nos muestran a la información que poseen sobre nosotros. Se es tima que el uso y capitalización de esta información todavía es superficial, pero aun así ha conseguido que Google se sitúe como la segunda empresa del sector tecnológico en capitalización bursátil, obteniendo el 99 % de sus ingresos de este incipiente mercado de publicidad dirigida.[124] ¿Qué podrán conseguir cuando logren ir un poco más allá en el uso de esta información? El día que se consiga utilizar las bases de datos, la explosión va a ser tremenda; y es tan sólo cuestión de tiempo que alguien encuentre el modo de rentabilizar la información que vamos cediendo poco a poco.

Y visto el papel que se le anticipa a esta información personal, parece inevitable que todos quieran acceder a esta información. Al fin y al cabo, todos esperan dar con la llave que permita lanzar toda una nueva gama de productos

personalizados, publicidad segmentada hasta lo individual y donde la cesión de parte de nuestra información personal sea un requisito necesario para acceder a la contratación de ciertos servicios: algunas aseguradoras ofrecen «ventajas» si consientes en llevar un detector GPS contigo cada vez que te pones al volante.[125] En el fondo, el enfoque es bastante diferente: las compañías de seguros están penalizando a aquellos que no se dejan espiar. Y ahora vayamos un paso más allá para ver qué podría ser mucho peor, pues de momento estos planes son opcionales pero, ¿qué sucedería si aquellos que no se dejan espiar no consiguen contratar un seguro? ¿Serán tratados como parias por querer mantener su privacidad? La política del miedo nos enseña a desconfiar de todos los que no actúan como la mayoría, así que ese futuro no es descartable. Si consideramos que estas imposiciones nos alcanzarán a todos, hay motivos más que suficientes para no entregar información personal a la ligera. El negocio de las bases de datos es la revolución comercial, económica y social (por todas las implicaciones que lo anterior imprimirá en el modo en que gestionamos nuestra vida) que está por venir; en estas circunstancias salvaguardar nuestra información personal y escoger adecuadamente a quién le damos el privilegio de conocerla

es un hábito que debemos desarrollar cuanto antes.

En la actualidad tenemos sistemas que funcionan con software libre y hay un fuerte movimiento de cultura libre que gana adeptos a cada minuto, pero la verdadera lucha en este momento es la lucha por la información personal y por su propiedad. ¿A quién pertenecen las bases de datos que construimos entre todos con nuestra información personal? ¿Quién puede hacer qué con nuestros datos, en qué condiciones y por cuánto tiempo? Sobre todo, ¿qué información no se nos puede obligar a facilitar bajo ninguna circunstancia (genética, historial médico, sistemas de vigilancia y seguimiento para acceder a seguros médicos o de conducción)? Necesitamos regular el hecho de que cuando yo abandono un servicio web para siempre se me permita no sólo a exportar todos mis datos, sino a obligar a la compañía a eliminarlos completamente de su base de datos. Eso sería libertad; todo lo demás genera una posición ventajosa para el prestador de un servicio y le proporciona una gran cantidad de información a cambio de prestar un servicio que, en la mayoría de casos, ya estamos pagando con nuestro propio dinero (lo cual equivale a decir que, en la mayoría de casos, estamos dando nuestra información a

cambio de nada).

La lucha en los días por venir no es por el software y la cultura libres, aunque sean luchas que deben continuar, sino por la propiedad y la privacidad de los datos personales.

La migración a la web

Debido a todos los motivos expuestos anteriormente, la migración a la web es algo que debe meditarse. En la web las opciones de software libre no están, en muchos casos, a la altura de las propietarias y es un frente en el que volvemos a caer cautivos del código que no nos dan. Además, en la web la privacidad se pone en peligro de forma innecesaria, pues muchas tareas para las que recurrimos a servicios web no mejoran nada nuestra experiencia con respecto al trabajo clásico en el escritorio. Por último, en la web, la relación proveedor-usuario es aún más radical que en la industria del software privativo tradicional: el proveedor controla tanto el código como los datos.

Y lo cierto es que, a pesar de todos los inconvenientes mencionados, la experiencia de comunicarnos a través de la red es muy interesante para la

mayoría de nosotros, por lo que plantear un rechazo absoluto de la misma quizá no sea la mejor respuesta. La respuesta, como siempre, está en mantener en lo posible las ventajas de ambos entornos: la ubicuidad de la web y el control que nos ofrece el escritorio. ¿Es esto posible? Solamente si decidimos montar el servidor en una máquina de nuestra propiedad albergada en nuestra propia conexión. No parece viable. Sin embargo, es posible encontrar un compromiso entre ambos sistemas.

Y el compromiso está, como no podía ser de otra manera, en el uso de herramientas libres en un servidor que, aunque no esté físicamente en nuestra casa, al menos sea un servidor controlado por nosotros de forma independiente. La migración a la web sólo es una opción válida si se realiza la migración hacia servicios libres que podamos tener bajo nuestro control, minimizando la dependencia de terceras partes y minimizando el acceso ajeno a la información personal que deseemos mantener bajo control. No podía ser de otra manera si tenemos en cuenta que cuando nos planteamos este tipo de cambios el principal factor a considerar es la defensa de nuestra privacidad.

5.10. Mucho trabajo por hacer

Visto todo lo anterior, resulta obvio que sería un error imperdonable caer en el triunfalismo de pensar que en la lucha del software libre ya está todo hecho y que la victoria de estos movimientos pro-libertades está asegurada. Aunque el software libre está cada vez más extendido y aunque es más la gente que considera importante gozar de y utilizar un sistema que no está limitado en cuanto a lo que se puede hacer con él, el resultado aún no está decidido. La concesión en la Unión Europea de patentes para desarrollos de software, algo que ya está permitido en Estados Unidos y que la gran industria del software privativo trata de introducir también aquí, podría crear muchos problemas al software libre. Las patentes abrirían las puertas a costosísimos litigios en los que las legiones de carísimos abogados que la mayoría de pequeñas empresas y desarrolladores independientes de software libre no podrían costearse acabarían barriendo todas las patentes para las casas de unas pocas y mastodónticas macroempresas.

De modo similar, el que el movimiento por una cultura libre consiga cada vez más adeptos y el que cada vez más personas creen sus obras y las liberen bajo licencias

libres no garantizan que esta tendencia se vaya a imponer en la sociedad y, sobre todo, no garantizan que las leyes vayan a reflejar esta evolución social desde la restricción de copia hasta la difusión de copias. Más aún, si hacemos recuento de todas las reformas legales acontecidas en los últimos años, se restringe cada vez más la copia y se favorece la creación de un ecosistema restrictivo y de escasez.

Por eso hay que evitar por todos los medios creer que estos sistemas se van a imponer mientras nosotros no hacemos nada. De hecho, los mismos medios que hace medio siglo se empleaban en la Unión Soviética para impedir que se copiase información (como poner un vigilante perpetuo en cada máquina capaz de hacer copias) se utilizan actualmente (cargar los sistemas con restricciones digitales). Y la dureza con la que la ley se aplicará para impedirlo será idéntica, como ya pudo comprobar Jamie Thomas, multada en Estados Unidos con unos 222.000 dólares[125] por compartir en Internet 24 canciones,[126] ya que se trata de un acto ilegal en este país. Resulta evidente que tampoco en este ámbito el futuro de las libertades digitales está garantizado.

6. Privacidad y publicidad

Cuando hablamos de privacidad hay dos aspectos básicos que pueden ayudar a erosionarla. El primero es la vigilancia en su sentido más amplio, que ya hemos comentado ampliamente en capítulos anteriores y cuyo abuso afecta a nuestras libertades. El segundo es la publicidad. Las nuevas técnicas de venta recurren cada vez más a un conocimiento intensivo de los hábitos de consumo y las aficiones del cliente, así como a su historial o su contexto.

Para ello los publicistas desarrollan y aplican métodos que les permiten conocer íntimamente a las personas. Si bien este uso no está relacionado directamente

con nuestras libertades, no deja de ser incómodo que alguien pueda saberlo todo sobre uno. Además, una vez que se recopilan los datos, nada impide que éstos sean solicitados por un gobierno o sean objeto de usos fraudulentos, por lo cual tampoco se puede desvincular la publicidad del primer aspecto ya comentado.

6.1. La sociedad en red y las marcas puras

La sociedad digital y el enorme peso específico que la información adquiere en el mercado de valor de nuestra economía permiten el afianzamiento del fenómeno de las marcas, surgido a finales del siglo XIX y que se caracteriza por el hecho de que dos productos idénticos tienen un precio diferente dependiendo de la marca que los avale. La marca actúa añadiendo valor de mercado al producto. Este fenómeno comienza a adquirir importancia en la segunda mitad del siglo XX, pero tendrá mayor relevancia en la sociedad digital y sobre todo en la red, donde las marcas ganan una preeminencia sin precedentes desvinculándose por completo de los productos que venden. Es lo que se denominan «marcas puras» y un par de ejemplos muy claros son Amazon e eBay.[127]

Pese a todo el valor que se le concede a lo digital y al nacimiento de las marcas puras, conviene recordar que incluso estas marcas puras como Amazon e eBay basan su modelo de negocio no en la producción y venta de bienes intangibles, sino en la compra, venta y envío de bienes físicos. Es importante considerar que apenas hay ejemplos de éxito en el comercio con bienes intangibles, si exceptuamos los bienes destinados al consumo de tiempo libre como videojuegos. E incluso en este caso habría que definir lo que consideramos un éxito comercial, ya que por más que disfruten de enormes campañas publicitarias de apoyo, aún no se ha dado el caso de alguien que se haya labrado una fortuna física comerciando con bienes inmateriales en videojuegos como *World of Warcraft* o Second Life, e incluso el número de personas que realmente comercian con objetos electrónicos pertenecientes a estos universos virtuales para obtener dinero real se puede considerar anecdótico en relación con el número real de jugadores.

Esto es así porque no se conoce un modelo de negocio sostenible basado en este tipo de sistemas: al menos de momento, parece que nadie podrá hacerse rico en el

mundo real vendiendo fortunas electrónicas; el fracaso mercantil entre el mundo virtual y el mundo real de Second Life está asegurado, aunque seguramente habrá legiones de jugadores que harán que su desarrollo sea un negocio rentable.

De lo anterior se que, incluso en un mundo donde la información es el activo de mercado más importante, la manufactura de bienes materiales seguirá siendo el motor de la economía. El comercio electrónico es electrónico sólo porque las peticiones se realizan de forma electrónica, pero los bienes que se mueven en este comercio son casi en su totalidad de carácter físico o una herramienta para conseguir esto último. Y sin embargo, las marcas que se generan en la red son marcas puras de productos intangibles. Amazon o eBay no tienen oficinas, no fabrican, pero se las asocia rápidamente con su actividad y nadie duda del valor añadido que supone el apoyo de uno de estos dos nombres en el lanzamiento de un nuevo producto ni de la ventaja de aparecer en sus catálogos.

6.2. Las cuatro P y la quinta P

La publicidad tiene, en principio, consecuencias

menos dramáticas que la vigilancia del tipo «por su seguridad» o panóptica. No obstante, la erosión de la privacidad debido a las técnicas publicitarias cada vez más desarrolladas y extendidas que se apoyan en un conocimiento cada vez mayor de los gustos y hábitos del cliente supone un peligro y una molestia crecientes.

La publicidad siempre basó su estrategia en la "teoría de las cuatro P": producto, precio, posición y promoción; fabricar un buen producto, ponerle un buen precio, colocarlo en un lugar preferente y promocionarlo en todas partes. Desde hace ya un par de décadas, se ha añadido una nueva "P" a las anteriores para ampliar esta teoría: personas. Los vendedores decidieron que para seguir aumentando sus ventas necesitaban saberlo todo acerca de las personas.[128]

La idea de estudiar al cliente tiene mucho sentido: un carísimo portátil, una PDA de último modelo y un traje de seiscientos euros podrían estar definiendo a un ejecutivo, mientras que ropa deportiva y un iPod podrían estar definiendo a un joven o un estudiante. Como la capacidad adquisitiva de ambos y sus posibles caprichos serán muy diferentes, la manera de presentar el producto también

debería serlo si se quiere optimizar la venta.

El gran escollo a la hora de luchar contra estas técnicas cada vez más invasivas es que, debido a su carácter pretendidamente inocuo, la forma en que nos enfrentamos a la publicidad es mucho menos beligerante que la forma en que nos enfrentamos a los sistemas de vigilancia «policial». El rechazo que nos produce es menos profundo, y muchas personas incluso aceptan esta intromisión en su intimidad. A menudo, cuando nos encontramos con publicidad nos limitamos a cambiar de canal. Otras veces intentamos rescatar la pieza útil de correo que nos llega entre océanos de publicidad no solicitada sin perder demasiado tiempo.

6.2.1. Publicidad personalizada

El fin último de añadir una quinta "P" a la estrategia clásica del publicista es tener la capacidad de desarrollar campañas publicitarias adaptadas a cada uno de los posibles clientes. Mediante esta acción se persigue mostrar el anuncio sólo a personas que estén interesadas en nuestro producto, reduciendo costes publicitarios y aumentando el rendimiento de las campañas. Es lo que se conoce como publicidad personalizada, segmentada o dirigida.

El objetivo final es conseguir que gastemos más dinero, y para ello pretenden ofrecernos anuncios altamente eficaces, que idealmente serían totalmente personalizados, aunque generalmente se limitan al diseño segmentado de las campañas: anuncios dirigidos a grupos o colectivos de personas agrupadas en función de un criterio arbitrario.

El principal problema de este tipo de publicidad no es sólo que únicamente beneficia al publicista y al producto que trata de vender, gracias al mayor éxito de una campaña publicitaria eficazmente confeccionada, sino que para que esta campaña dirigida se produzca tendremos que proporcionar al publicista suficiente información sobre nosotros. Esta información permitirá al vendedor realizar un «retrato robot» de nuestros gustos, costumbres y/o situación actual: le permitirá trazar nuestro perfil.

6.3. Trazabilidad y perfiles de consumidores

La trazabilidad es la capacidad de realizar el vínculo entre una determinada persona y sus actividades, opiniones o adquisiciones. Si nos restringimos únicamente a los usos publicitarios, la trazabilidad es la posibilidad de vincular a

una persona con sus compras, de forma que se pueda obtener un conocimiento amplio de la persona estudiando qué cosas consume, con qué frecuencia y en qué circunstancias. Si hablamos de trazabilidad en la red, es la capacidad de saber en todo momento quién se conecta a qué servicios, conocer las actividades en la red de las personas, en ocasiones vinculándolas con la persona física.

La trazabilidad permite la obtención de completos perfiles personales que los vendedores pueden utilizar para adaptar mejor sus campañas de publicidad segmentada y para estimar, por ejemplo, la capacidad adquisitiva de alguien a partir de los pagos realizados con tarjeta.

6.3.1. Tarjetas de comprador frecuente

No hay nada que favorezca más la trazabilidad de nuestras compras que el hecho de pagar con tarjetas. Existen dos tipos de tarjeta muy extendidos que nos ayudan a pagar nuestras compras: las tarjetas de crédito y las tarjetas de comprador frecuente.

Las tarjetas de crédito nos las ofrecen nuestras entidades bancarias y sirven para no llevar una cantidad excesiva de dinero en efectivo. Son un medio para comprar

sin arriesgarnos a que un robo o una pérdida asesten un serio golpe a nuestros ahorros. Aunque no resulte recomendable pagar con ellas cantidades pequeñas, por lo que supone de exposición al fraude y porque facilitan la trazabilidad de nuestras compras, no cabe duda de que las tarjetas de crédito tienen beneficios cuando se trata de compras de valor elevado.

Sin embargo, resulta complicado delimitar estos mismos intereses cuando hablamos de las tarjetas de fidelidad, también llamadas de "comprador frecuente". La tarjeta de crédito es práctica porque nos evita llevar elevadas cantidades de dinero en efectivo, pero ésta actúa de otra manera. Usada junto a una tarjeta de crédito, la tarjeta de comprador frecuente ofrece al comercio, generalmente un supermercado, mucha más información de la que ofrecemos al banco. Esta información se entrega habitualmente a cambio de nada: ningún beneficio real. Existen compañías que se dedican a almacenar información sobre las compras realizadas en supermercados con ayuda de la información recogida en las cajas. Desde 1987, Information Resources Inc. se dedica a la acumulación de información sobre compras. Se estima que a principios de

2005 el tamaño de las bases de datos de IRI rondaba los 460 terabytes.[129] Igualmente, se estima que en 2004 el tamaño de las bases de datos de Wal-Mart era aproximadamente el doble del tamaño de Internet.[130] Tres años después, con una red de cajeros «inteligentes» cada vez más extendida, no cabe duda de que esa información será mucho mayor: todo queda registrado, y eso significa que cada compra que hacemos, cada yogur, cada pan, cada perfume, le dice al comerciante quiénes somos y qué consumimos. Cada compra enseña al comerciante a vendernos mejor.

Las tarjetas de comprador frecuente surgen con la promesa del ahorro. Comprar repetidamente en un supermercado generaría algún tipo de descuento o permitiría acceder a ofertas especiales o personalizadas. Así visto, parece que el comprador sale ganando si emplea esta tarjeta. Pero un análisis profundo de la situación nos lleva a descubrir que, gracias al historial de compras, la información que posee el comerciante (qué compra, en qué cantidades y con qué frecuencia, si responde a las ofertas comprando los artículos...) le permitirá optimizar la manera en que presenta su oferta al cliente, generando un mayor deseo y consiguiendo que éste compre más artículos de los

que habría comprado con una oferta genérica. De esta forma, el gasto final se dispara por encima de lo que planeábamos y descompensa la cuenta de ahorro hasta el punto que al supermercado le resulta enormemente rentable entregar este tipo de tarjetas. Esto no debería sorprender a nadie, ya que estamos hablando de publicidad: el objetivo es siempre separar a la gente de su dinero.

6.3.2. RFID y publicidad

¿Qué vínculo existe entre la identificación mediante radiofrecuencias y la publicidad? Con lo que ya conocemos sobre RFID, el vínculo es la trazabilidad que esta tecnología hace posible. La RFID se comporta como una formidable herramienta de generación y acumulación de información acerca de las personas, y supone un punto de ruptura con todo lo que la publicidad ha sido hasta ahora. La RFID abre una puerta a la publicidad completamente personalizada, en la que cada persona recibe un mensaje único y totalmente adaptado a ella debido al identificador único que porta: las etiquetas RFID que hacen posible estos mecanismos de personalización.

A menudo comparadas con el código de barras, las

etiquetas RFID presentan una capacidad que las diferencia radicalmente de éste: el código de producto electrónico (EPC) específico para cada artículo y que no sólo informa de qué compras se realizan (eso ya se sabe cada vez que pagas una compra con una tarjeta de crédito o con una tarjeta de comprador frecuente), sino que informa también de cómo y cuándo se consumen. Incluso de cómo se compra, si uno se detiene delante de la estantería mucho tiempo o poco, si luego va a comparar con otros productos similares, si reacciona ante los carteles de «oferta» deteniéndose y leyendo más y cuánto tiempo dedicas a estos carteles.

Para realizar todo este seguimiento hacen falta lectores de RFID. Claro que actualmente no hay muchos lectores por todas partes, pero no hay que olvidar que los componentes electrónicos para fabricar uno de estos dispositivos no cuestan más de 100 euros (siendo conservador); estoy seguro que alguien que quiera fabricarlos y compre cientos de miles de componentes pagará mucho menos e incluso podrá venderlos por mucho menos. Piensen que, por ejemplo, tampoco hace falta sembrar de lectores la ciudad ni el supermercado. El supermercado es un área pequeña y la inversión de poner

lectores en los pasillos no es desorbitada si se tiene en cuenta la información que permitirán recolectar.

Quizá lo que más sorprende a los que descubren estas aplicaciones es que las aplicaciones publicitarias de la RFID no sólo se centran en el supermercado, sino que están diseñadas para invadir las calles y llegar hasta nuestro hogar. Un ejemplo clásico lo encontramos en *Minority Report*. En esta película hay un momento en que el protagonista corre a través de un pasillo para llegar al metro y una pancarta publicitaria le ofrece a él, específicamente a él, una cerveza de una marca conocida. Con la RFID se puede conseguir que los monitores publicitarios que cada vez van sustituyendo a las vallas estáticas muestren anuncios diferentes según quién se posiciona delante de ellos y según los objetos que lleva. La misma idea ha sido aplicada al mundo real por el fabricante de automóviles Mini, que regaló a los compradores de sus vehículos un llavero RFID para que pudieran observar anuncios personalizados al circular por las carreteras.[131]

Aquellos que no ven en esta tecnología un problema que les haga oponerse a la misma afirman que quizá la construcción de un perfil por parte del comerciante permita

recomendar nuevos productos que de otra forma no se descubrirían. La pregunta es, ¿está usted dispuesto a pagar el precio por disfrutar de esos mensajes adaptados a su persona? Para que el fabricante tenga la posibilidad de ofrecerle anuncios personalizados que realmente coincidan con sus intereses y con lo que usted puede pagar necesita disponer de tanta información sobre usted como para poder trazar un perfecto perfil de su persona. Toda esta información se acumula en grandes bases de datos como las que hemos mencionado de Information Resources Inc. Y esta tendencia no hará sino aumentar vertiginosamente en los próximos cinco años, acercándose cada vez más a los anuncios individuales completamente personalizados, según predice un reciente estudio de IBM.[132]

6.3.3. Publicidad en la red

La red es una fuente inagotable de información acerca de las personas: patrones de comportamiento, aficiones, rutinas, relaciones sociales. Desde un principio estuvo claro que esto no iba a pasar inadvertido a los publicistas. Y sin embargo es algo que la mayoría de las personas que entran en la red no se plantean jamás.

Nuestra navegación por la red siempre deja registro en alguna parte. Destacaremos el caso de las webs en las que estamos registrados. Estas webs acumulan información sobre nosotros (cuándo entramos, con qué frecuencia, quiénes son nuestros contactos, qué compramos en ellas, nuestra agenda). Esta información normalmente está vinculada a nuestro correo electrónico y quizá a nuestra información bancaria. Constituye una fuente primaria de información sobre nosotros y es por tanto un activo de mercado: algo con lo que se puede comerciar. Precisamente, mercadear es algo que hacen la mayoría de los sitios webs con la información que poco a poco les vamos proporcionando; y eso es precisamente lo que más del 50 % de los usuarios no ha comprendido todavía, según Chris Hoofnagle (Samuelson Clinic, Universidad de Berkeley).[133]

El valor de la información personal

Aunque las personas creen que los datos que se guardan sobre ellas cada día en la red o los que entregan a una empresa determinada no se van a utilizar para comerciar con ellos (venta a terceros, publicidad dirigida), esto es lo que sucede en la mayoría de los casos. No es sólo que el servicio sea gratuito porque el sitio se mantenga

gracias a un determinado acuerdo publicitario, es que lo más probable será que ese sitio web use la información que posee sobre sus usuarios como un activo susceptible de ser vendido, alquilado o cedido previo pago y en determinadas circunstancias.

Ya hemos mencionado cómo Chris Hoofnagle llega a la conclusión de que más de la mitad de los usuarios de la red tiene una percepción completamente equivocada de este asunto. Para ello hay que entender que el sistema de publicidad dirigida más exitoso hasta el momento es el desarrollado por Google, Google AdSense/AdWords. Este sistema permitió a Google ser la segunda empresa por capitalización bursátil dentro del sector tecnológico a finales de octubre de 2007,[134] a pesar de estar aceptada mayoritariamente la percepción de que los anuncios dirigidos o segmentados aún son algo en lo que casi todo está por descubrir, algo de lo que Google tan sólo araña la superficie.

De todo esto lo único que podemos deducir es que las bases de datos con información personal tienen un valor muy elevado, difícil de estimar actualmente, pero muy elevado en cualquier caso. De ahí que una de las mayores

tendencias que se dan en la red actualmente sea incentivar la migración al uso de aplicaciones en línea y el nacimiento de lo que se denominan *webs sociales*: sitios web en los que el usuario crea un perfil con información propia (datos personales, aficiones, gustos, amigos), de forma que pueda contactar con personas con un perfil similar o con las que comparta ciertos intereses.

Sin entrar a evaluar si estas webs sociales son buenas o malas, no podemos ignorar que el objetivo final de muchas de ellas es recopilar tanta información de los usuarios como sea posible, incluso pactando con terceros (otros sitios webs) para completarla, si fuera necesario, como es el caso de Facebook.[135] El negocio en torno a la publicidad personalizada se estima tan grande que ninguno de los actores principales del sector se quiere quedar fuera, como ocurre con Microsoft, que presentó un sistema de publicidad personalizada, The Colonel, que mostrará publicidad contextual relacionada con el contenido de tu disco duro,[136] en otro intento de violación flagrante de nuestra privacidad.

Y sin embargo, al hilo de esta situación surge una cuestión interesante: ¿quién es el dueño de los datos? ¿De

quién son las bases de datos? ¿Puede un usuario de un sitio web sencillamente recoger sus cosas e irse a otra web sin que la empresa pueda mantener una copia de su información confidencial? Al fin y al cabo, si dejo de utilizar el servicio, ¿por qué la web puede quedarse con mis datos? Estamos de acuerdo en que un sitio web ofrece un servicio, generalmente gratuito, que financia y rentabiliza insertando publicidad. Sin embargo, el sitio web hace negocio recogiendo una cantidad de datos del usuario que en muchos casos abarcan espacios reservados de su vida privada, muchas veces sin que el usuario sea consciente de que toda esa información se está recogiendo. ¿Quién es el dueño de los datos? Habitualmente se ponen trabas al completo control de los datos por parte de sus usuarios, y aún en el caso de que éstos puedan llevárselos a un sitio web, nada hace pensar que el viejo servicio vaya a eliminar toda esa información que le permitirá seguir mercadeando. Claro que la Ley Orgánica de Protección de Datos obligaría al prestador de servicios a eliminar toda la información personal que solicitemos borrar, pero ¿qué porcentaje de webs operan desde España y se acogen a nuestra LOPD?

Mientras toda esta situación se normaliza de la

manera que se deben hacer las cosas, que es legislando al respecto, lo único que nos queda es nuestra propia prudencia. La información personal está muy cotizada en el pujante mundo de la publicidad en la red. Antes de entregarla a un nuevo sitio web es saludable analizar el canje y evaluar si estamos recibiendo a cambio un servicio suficiente que justifique entregar esa porción de información que se nos reclama, o si aquello que el servicio web nos ofrece se puede obtener por otras vías que no requieran entregar esa información y estamos regalando una información valiosa con la que alguien se va a lucrar. Porque hay algo que de tan sencillo que es se nos olvida, pero no deja de ser importante: si todos registran datos sobre nosotros, y en unos tiempos en que todo queda grabado en alguna parte, es porque todos piensan utilizar esos datos. De una forma u otra todos piensan sacar provecho de lo que les decimos con cada pasito que damos en la web.

6.4. La captura de espacios públicos. Publicidad en las calles.

Tradicionalmente las ciudades han sido espacios para el disfrute y desarrollo de la vida pública y privada. Las

ciudades nos pertenecían y en ellas, especialmente en países con climas suaves y apacibles, como el mediterráneo, transcurría gran parte de nuestras actividades. La ciudad en la que crecieron mis padres, y aquella que yo conocí de pequeño, estaba llena de lugares para pasear y disfrutar en compañía. Como toda ciudad tenía sus peculiaridades.

Las ciudades, sin embargo, experimentan una transformación cada vez más acelerada que les roba su esencia. La utilización publicitaria de nuestras calles es cada vez mayor y refleja una ambición sin límites. Luces de neón, vallas publicitarias. Las áreas comerciales de la ciudad, típicamente los cascos antiguos, se convierten en lugares estruendosos durante el horario comercial que se quedan súbitamente desiertos cinco minutos después del cierre. La gentrificación de los barrios típicos y la espectacularización de los mismos no dejan lugar para el simple ciudadano que quiera disfrutar la ciudad. No hay lugar para el ocio si no va ligado al gasto económico directo.

Las ciudades se han convertido en enormes supermercados donde todo vale con tal de colocar un anuncio ante los ojos de todo el mundo. Las tiendas no apagan sus luces, ni siquiera de noche, cuando por obra y

arte de esos mismos comercios nadie transita, pues en una calle plagada de locales cerrados no hay nada que hacer. Los edificios están coronados por enormes letreros que podrás ver desde cualquier parte, y cada vez más, ciudades enteras ceden ante esta invasión publicitaria de altura.

Pero no sólo los edificios, también los trenes, los autobuses públicos o los servicios de bicicletas municipales de alquiler (que, por cierto, incluyen chips RFID) se han convertido en enormes –no tan enormes en el caso de las bicicletas– vallas publicitarias. Un autobús podría ir disfrazado de chocolatina o de la última película de acción estadounidense. Un autobús público, costeado doblemente por todos nosotros -impuestos y billete de viaje-, sirve para continuar alienándonos de nuestra ciudad, cuyas calles se convierten poco a poco en un mal necesario, siempre desde el punto de vista del vendedor: un pasillo inevitable que separa nuestra casa de sus tiendas, nuestro bolsillo de sus cajas registradoras.

Y esta situación no hace sino empeorar día a día mientras avanzamos hacia el modelo de la ciudad espectáculo. Una ciudad sin alma que se disfraza de algo cada cierto tiempo. Ejemplos de este tipo de desarrollos son

el Forum de Barcelona o el Millenium Dome de Londres, que pretendían conferir a estas ciudades un aura que les era absolutamente ajena y que nada tenía que ver con la historia de la ciudad. Pero sin duda alguna, el caso más espectacular de esta nueva ciudad espectáculo lo encontramos en Lille (Francia) de la mano de Lille 3000.

Lille 3000 es un proyecto que se autodenomina cultural y que pretende transmutar la ciudad cada cierto tiempo para ofrecer un nuevo marco decorativo. Una especie de "Ocho días dorados a lo Corte Inglés", pero invadiendo para ello las calles, robando virtualmente el espíritu de la ciudad a sus habitantes, a cambio de un negocio continuo del que unos cuantos comerciantes sacan buena tajada,[137] mientras la mayoría de los ciudadanos de Lille sólo consigue unos precios más elevados a causa del potencial turismo y la pérdida del espíritu de su ciudad.

Evidentemente, se plantea como algo prioritario, de importancia enorme, la recuperación de los espacios públicos para uso público y, dentro de lo posible, libres de publicidad. En Sao Paulo (Brasil) la recuperación de espacios públicos es una realidad, ya que en septiembre de 2006 se aprobó una ley que prohibía la colocación de vallas

publicitarias en la vía pública. En junio de 2007 ya se apreciaban los efectos de esta reforma que, según los que la vivieron, hizo de la ciudad un lugar mucho más sereno.[138] Las panorámicas que pudimos ver entonces resultaban chocantes para los que estamos acostumbrados a convivir con paisajes urbanos de neón; las panorámicas que pudimos ver entonces se antojaban preciosas, envidiables, para los que no tenemos más remedio que vivir rodeados de vallas publicitarias.

Supongo que Sao Paulo es el modelo de ciudad pesadilla para los publicistas de nuestro tiempo, pero creo que, quizá sin llegar a esos extremos, sería magnífico que una regulación limitara el uso (y el abuso) de la publicidad en la vía pública. Hace falta reclamar los espacios públicos que nos han arrebatado, pues son esos espacios los que hacen que nuestras ciudades sean algo único y diferente.

6.4.1. La ciudad supermercado: RFID en las calles

Es una de las ambiciones de los publicistas, y también uno de los motivos de que consideren la tecnología de identificación mediante radiofrecuencias como "lo más grande desde que Edison nos dio la bombilla".[139] La

ocupación de las calles hasta convertirlas en masivos centros comerciales es algo que ya ha comenzado. Y llegará el momento en que ese supermercado callejero esté completamente cubierto por chips RFID, aunque de momento no haya más que pruebas piloto.

Para que este sistema funcione es necesario que cada transeúnte esté dotado de un sistema emisor-receptor de RFID, de modo que su posición sea monitorizada en tiempo real por los comercios más cercanos a su posición. Estos comercios podrían usar la información obtenida del transeúnte (qué ropa lleva, qué zapatos, qué modelo de teléfono o PDA), gracias a los chips RFID que estos productos incluyen, para enviar publicidad específica al mismo.

Esto ya se ha hecho con el *bluetooth* y los teléfonos móviles, pero habría que resaltar algunas diferencias importantes. La primera es que el *bluetooth* de los teléfonos lo apagamos a voluntad, deteniendo así la entrada de publicidad. Las etiquetas RFID no las podemos desactivar, y la puerta para la publicidad siempre está abierta. Quizá podamos apagar el dispositivo que nos permite leer la publicidad, pero eso no cambia otro hecho muy importante y muy diferente: las etiquetas RFID ofrecen mucha más

información que la simple disponibilidad de un teléfono con *bluetooth* activado y permiten acumular información sobre nosotros incluso aunque no se usen inmediatamente. Si alguien lleva puestos unos Levi's (equipados con una etiqueta RFID) en la tienda sabrán que es mejor enviarle publicidad de vaqueros que de ropa deportiva, por poner un ejemplo. Como cada vez que entras la información es almacenada en tu perfil, con el tiempo la tienda sabrá exactamente qué te gusta comprar y qué anuncios debe mostrarte para que su publicidad cumpla el objetivo fijado (que gastes más dinero). Estos sistemas ya han sido probados en algunas ciudades de Japón en el marco del Tokyo Ubiquitous Network Project.[140]

La promesa es siempre la misma: publicidad personalizada a tus gustos. Y nadie repara en analizar a quién favorece o perjudica esa publicidad personalizada. La publicidad personalizada es un invento genial para los vendedores, no para los clientes. El trasfondo de estos movimientos es siempre el mismo: publicidad cada vez más invasiva para convertir las calles de la ciudad en un enorme centro comercial. Lo que antes eran calles para pasear y leer, ahora son zonas para comprar entre el bullicio y volver

corriendo a casa cuando te quedas sin blanca.

6.5. La captura de espacios privados. Publicidad en el hogar

Nuestro hogar es hoy por hoy el único espacio libre de publicidad que tenemos. Y eso considerando que la televisión y sus rítmicos anuncios inundan las salas de nuestra casa, o que Internet es también una gran entrada de publicidad en la intimidad de nuestro hogar. Pero al menos no se nos muestran anuncios, todavía, cuando sacamos algo de nuestro frigorífico o abrimos el armario. Eso podría cambiar con la RFID. El hogar también está en el punto de mira de los publicistas, pues es una vía magnífica para conocer profundamente a sus clientes potenciales.

Contra lo que pueda parecer, para analizar los hábitos de una persona no hace falta plagar de lectores RFID su hogar: un par de ellos serán suficientes y próximamente vendrán integrados en los electrodomésticos, como en los frigoríficos,[141] los mismos que ya podemos ver en numerosos hoteles.[142] Estas neveras ofrecen la opción de la RFID como mecanismo de control e inventario casero de productos. De esta forma sabrá cuánto queda de un producto (o si éste se

ha agotado) y, si se lo permiten, hará un pedido automáticamente al proveedor preferido.

Esto, que parece una comodidad, le sirve al supermercado y a sus publicistas para conocer exactamente cómo consume una persona sus productos. Si se combinasen las bases de datos de su proveedor de televisión digital (que conoce en cada momento qué está viendo en la televisión) y de su supermercado, podrían averiguar cuál es su bebida preferida para cada programa de televisión, de forma que ambos optimizarían sus anuncios (por ejemplo, ofreciendo productos similares) para conseguir que se gastara más dinero del que, quizá, habría gastado de forma natural.

El verdadero problema es que, con estos elementos, La inocencia y el carácter íntimo de los actos que realizamos cuando estamos en casa desaparecen, ya que cada paso que damos, cada vez que abrimos la nevera o el botiquín, estamos enseñando a alguien cómo somos: una diminuta ventana a nuestro interior o, para ser precisos, infinitas diminutas ventanas a nuestro interior.

6.6. Todo esto, ¿es bueno o malo?

El motivo por el que las aplicaciones de la publicidad

personalizada pueden ser negativas es la gran información que se necesita obtener de las personas para que ésta sea efectiva. Estos sistemas están diseñados para conocer todo acerca de cómo se utilizan los productos, con la intención de acumular conocimientos sobre las personas, y por eso las bases de datos que se generan tienen un potencial de uso no equilibrado, en el sentido de que el beneficio para el usuario no compensa la pérdida que le supone toda esa entrega de información.

De hecho, las probabilidades de uso no apropiado de todo ese rastro que vamos dejando son tan altas, que ya en sí mismas justifican el rechazo a la utilización de la mayoría de estos sistemas. Tal extremo, el rechazo dogmático de esta publicidad, tampoco es una aproximación correcta al problema. Lo ideal es evaluar por separado cada sistema atendiendo a diversos parámetros: qué información se nos pide y en cuánto valoramos la misma, podemos activar cuándo permitimos o no que funcione el sistema o requiere estar activado permanentemente, qué beneficios nos aporta. Sólo así podremos tomar la decisión correcta, y esa decisión correcta, si nos atenemos al ámbito de la publicidad, puede ser diferente para cada uno.

Sin embargo, mi opinión es que el servicio que ofrece la mayoría de ellos no compensa si se tiene en cuenta lo que piden, debido al elevado valor que para mí tiene la información personal que me solicitan a cambio. Entre los principales motivos para rechazar esta nueva manera de entender la publicidad está nuestra intimidad: nuestro hogar es hoy por hoy (y cada vez menos) el único espacio libre de publicidad que tenemos. Si nuestra nevera es capaz de detectar cuándo falta leche, de comprarla e incluso de ofrecernos unas magníficas galletas de chocolate para acompañar esa leche, estamos dando al publicista la oportunidad de gobernar el desarrollo de un acto cotidiano como es el de ir a nuestra cocina y prepararnos una taza de café.

Para obtener la ventaja más que cuestionable del aviso automático con una información que podemos ver cada vez que abrimos la nevera y un anuncio de un producto relacionado, algo que sigo sin ver como una ventaja, debemos entregar a una empresa privada tanto una gran cantidad de información sobre nosotros como la capacidad de comerciar con nuestros datos (algo que podría ir incluido en el contrato de prestación de servicio). La unión de estos

dos factores multiplica las posibilidades de usos inapropiados o indebidos de todos esos datos.

El quid de todo este asunto es valorar adecuadamente nuestra información y nuestra privacidad, para así decidir en qué casos estaríamos dispuestos a aceptar esta publicidad y en cuáles no. Asimismo, sería necesario regular jurídicamente áreas que no puedan ser invadidas bajo ningún concepto. No olvidemos que en lo que respecta a la privacidad existe un gran vacío legal, ya que se trata de un derecho civil contemporáneo que no ha sido necesario reclamar con anterioridad y cuyos aspectos se encuentran pobremente regulados.

6.7. Publicidad descontrolada, ¿dónde ponemos el límite?

Podemos hablar largo y tendido de las nuevas estrategias de la publicidad: la captura de espacios públicos y privados, la captura de nuestras actividades cotidianas y de nuestros hábitos, la segmentación de los anuncios. Todo ello nos llevará inequívocamente a una pregunta final: ¿quién debe poner límite a la publicidad? Ya podemos comprobar que, si nosotros no actuamos, los vendedores no

parecen tener el más mínimo reparo en invadir nuestra intimidad, quizá porque a ellos no les parece negativa la publicidad, sino que la contemplan como un modo de vida. Por tanto, es obligatorio hacerse una pregunta: ¿es conveniente dejar que sean los vendedores los que controlen la cantidad y la intromisión de la publicidad? ¿Hasta dónde debe llegar ésta? ¿Corre peligro nuestra intimidad?

Estas preguntas reflejan toda una problemática social que nace del drástico cambio que ha sufrido nuestra sociedad en los últimos años. Sobre quién debe poner límite a la publicidad y si debemos confiar en los vendedores, la respuesta es intuitivamente rápida: nosotros debemos ser capaces de decidir qué publicidad aceptamos y qué publicidad rechazamos; ser capaces de hacerlo técnica y legalmente. Del mismo modo que mientras navegamos por Internet aceptamos publicidad contextual y rechazamos la publicidad intrusiva, podemos aceptar una publicidad que cumpla su función, que no es otra que vender, sin apoderarse de nuestro entorno privado y rechazar vías publicitarias más agresivas que sí lo hacen.

Y es que los publicistas no pararán hasta llenarlo todo de anuncios: la web, la calle, nuestra casa. Porque

aunque esto no lo justifique, ser publicista consiste en vender tu producto a toda costa. De forma que aunque pueda parecer excesivo estudiar todos y cada uno de los hábitos de una persona con el fin único de venderle mejor, más que intentar convencer a los publicistas de lo ético o poco ético de este comportamiento, debemos analizar la situación y decidir nosotros mismos.

Si los anuncios son indiscriminados y no podemos evitar aportar información al publicista o recibir esos anuncios, no serán aceptables y habrá que rechazarlos. Si los anuncios son aceptados como parte de la prestación de un servicio con precio reducido, hay que valorar si la rebaja del coste compensa efectivamente. Sin duda hay servicios que no podrían existir en ausencia de publicidad (¿podría Google ofrecer el servicio de búsqueda que ofrece si no se sostuviera con publicidad?), pero quizá no hace falta aumentar hasta el límite la cantidad de información que Google (por continuar con el ejemplo) obtiene de nosotros para ofrecer su servicio. ¿Hasta qué punto compensa, en el sentido de cuánta información es justo entregar a cambio del servicio gratuito que se nos presta? Del mismo modo que el famoso buscador, multitud de servicios web ofrecen algo y se subvencionan

con la publicidad adaptada a nuestro perfil, publicidad que nos muestran en todo momento.

Antes de aceptar como inevitable el hecho de que todo servicio vaya inherentemente acompañado de un programa de publicidad segmentada, hay que analizar detenidamente las ventajas comparativas que se nos ofrecen y lo que nos cuesta, no en dinero sino en información personal, dicho servicio. La gran mayoría de servicios de este tipo no aprobaría una comparación de este tipo al evaluar la relación ventajas-información entregada.

De esta forma, es a nosotros y a nadie más a quien compete decidir qué servicios nos compensa usar y qué información entregamos a cada publicista. En este sentido, la tecnología RFID nos priva del control sobre el sistema, pues no se puede desconectar a voluntad, pero los pagos con tarjeta de fidelidad y la traza que dejamos pasan a ser responsabilidad nuestra. Del mismo modo, resulta difícil evitar que diversos servicios web almacenen información sobre nuestra navegación, pero mucha de esa información la entregamos gratuitamente al navegar sin cerrar nuestra sesión de trabajo en estos sitios o al completar un perfil con información personal que entregamos a cualquier servicio

web. Estos actos también son responsabilidad nuestra.

No quiero decir que la aceptación de esta publicidad sea algo descabellado; desde luego, tiene sus ventajas y sus posibilidades. Mi única reflexión es que a veces no tenemos suficientemente en cuenta como estos aspectos reducen nuestro espacio privado.

7. Derechos civiles digitales

Bajo el denominador común de derechos civiles digitales o ciberderechos se agrupa tradicionalmente la parte de nuestras libertades fundamentales que se relaciona con el uso de esta libertad en la red. Los derechos civiles digitales son, por tanto, los derechos civiles con que contamos cuando se trata de realizar alguna actividad en la red y son extremadamente importantes porque las libertades civiles contemporáneas no pueden permitirse un punto débil en la red, donde ya tiene lugar una gran parte de nuestra actividad cotidiana y donde, en muy pocos años, tendrá lugar la práctica totalidad de nuestras actividades diarias. Por tanto, los ciberderechos son mucho más que el

derecho a la privacidad, aunque nosotros le prestemos una atención mayor a éste.

Lo primero que hay que tener siempre en mente cuando uno habla de derechos civiles digitales, ciberderechos o, simplemente, derechos civiles es que estos derechos son los que nos permitirán afrontar con garantías el futuro en la sociedad en la que vivimos. Los ciberderechos son los derechos del futuro. Más aún, en la sociedad actual, dependiente de la tecnología digital, los derechos civiles digitales son ya tan importantes y tan irrenunciables como puedan serlo los derechos civiles en su forma clásica.

El objetivo que tenemos por delante y por el que habremos de pelear es equiparar socialmente estos derechos, poner fin a la separación tejida a medida desde el oligopolio político y económico y cuya finalidad es promover que estos derechos se perciban como algo secundario, un extra que se puede conceder a cambio de regalías. Lejos de ser algo accesorio y prescindible, no disponer de ciberderechos equivale a no tener derechos y con cada día que pasa sin que equiparemos estos dos conceptos, con cada ley que se aprueba para reducir los espacios libres digitales, estamos perdiendo las armas que nos ayudarán a mantener

nuestra sociedad libre en el futuro más inmediato. En un momento en que nos informamos y nos comunicamos más que nunca usando la red, disponer de leyes que permitan salvaguardar la libertad de expresión y de información en la misma equivale a luchar por el derecho a la libertad de expresión y de información en toda su extensión.

Ya hemos mencionado anteriormente que la privacidad es más que un problema técnico un problema legal. Siguiendo con este razonamiento, podemos decir sin miedo a equivocarnos que la batalla por la privacidad es, ante todo, una batalla legal. Y podemos concluir diciendo que la legislación existente no protege adecuadamente estos derechos. De una forma más precisa, la batalla por la privacidad es una batalla civil para conseguir una victoria legal: el reconocimiento oficial de una serie de derechos, de forma que se fortalezca la defensa de los mismos frente a las violaciones a las que actualmente están sujetos y que tienen lugar de forma más o menos impune. Estas violaciones serán más graves y más importantes en el futuro, en que está previsto que todo, absolutamente todo, esté conectado a la red, y regularlas e impedirlas es una labor básica en la tarea de reequilibrar la democracia para adaptarla a los nuevos

tiempos.

7.1. Tendencias

Las doctrinas políticas que parecen regir las tendencias legislativas de la Unión Europea, importadas directamente de Estados Unidos, y que más influencia tienen a la hora de definir las leyes que se van a adoptar en este ámbito no son nada favorables para los que queremos fortalecer estas libertades. En muchas ocasiones se legisla directamente en contra de nuestros derechos. Esta tendencia se ha agudizado desde el inicio de la «guerra contra el terror». En el resto de ocasiones, cuando no se legisla en contra, lo habitual es que no se legisle nada en absoluto, lo que posibilita la existencia de lagunas y vacíos legales importantísimos que constituyen un caldo de cultivo para nuevos abusos, como la ambigüedad con la que se definen determinados términos. Un ejemplo es la referencia a la «autoridad competente» introducida en la última Ley de Medidas para el Impulso de la Sociedad de la Información (LISI), aprobada en diciembre de 2007 y que desató un gran número de protestas contra los grupos parlamentarios y la clase política en general.

Las leyes que se elaboran sobre diferentes asuntos en nuestro país y en la Unión Europea están dictadas por los grupos de presión empresariales, generalmente estadounidenses, de los distintos sectores. Esto, que sucede pese a que en diversos asuntos la oposición social haya sido realmente notable, podría suceder incluso aunque nos organicemos y pidamos la rectificación y revisión de numerosas leyes. Sin embargo, la única posibilidad de saber si las instituciones democráticas que nos representan ignoran nuestra voluntad es recurriendo a dicha organización y haciendo llegar a las mismas todas estas peticiones.

De gran importancia resulta comprender que la sociedad digital ha revolucionado el modo en que funcionaban nuestras instituciones y ha modificado gran parte de los paradigmas que regían nuestro derecho. El cambio es tal, que se hace necesario un análisis de la nueva situación para poder adaptarnos al nuevo entorno sin que la estabilidad de nuestras democracias corra peligro. Los grupos de presión empresariales y políticos, oligárquicos por naturaleza, intentan trasponer el sistema anterior a la nueva sociedad digital, sin modificarlo ni un ápice; muchas

personas se han rebelado contra esta situación haciendo saltar los candados impuestos. Se podrá discutir si lo que hacen es legal o no, pero no parece descabellado que lo hagan: lo cierto es que la sociedad digital necesita leyes que la protejan y estabilicen, algo que en democracia se hace defendiendo los derechos de todos y cada uno de los miembros de la sociedad por encima del interés particular de uno o varios grupos concretos.

7.2. Notas sobre la «globalización»

La globalización, o lo que conocemos como globalización, es un proceso político que está teniendo lugar lugar desde la década de los setenta y que profetiza la creación de un único mercado global y libre como vía para promover un crecimiento económico global que haga posible la desaparición de todos los problemas económicos y sociales gracias a la labor terapéutica que los mercados y el comercio internacional ejercen en las relaciones internacionales. Como resultado de este pensamiento, toda reforma de las relaciones comerciales internacionales pasa por la eliminación de los impuestos transfronterizos, las aduanas, la rebaja de la presión fiscal y todo tipo de medidas que permitan que las mercancías circulen de una a otra

parte del mundo libremente.

El gran problema de la globalización es que lo único que ha globalizado son los mercados. La globalización ha conseguido facilitar el traspaso de mercancías de un país a otro y ha conseguido facilitar el traspaso de capitales de un país a otro, pero lo ha hecho para poder comprar barato a los productores del tercer mundo y venderles caro a los consumidores del primero, y para conseguir esto es importante que las personas no puedan circular libremente. La globalización ha globalizado todo excepto a las personas, que siguen atrapadas en sus diferentes rediles estatales. Como consecuencia de esto, la presión contra la inmigración aumenta constantemente en todo Occidente, ya que el cierre de las fronteras es el único mecanismo que mantiene la ilusión del mercader global: la de comprar barato en África y vender caro en Europa.

El problema es que lo que conocemos por globalización es en realidad una falsa globalización, pues no permite el libre movimiento de personas a través de los territorios. Permitir el libre movimiento de personas, tal y como ya sucede con los capitales y las mercancías, daría lugar a una verdadera globalización potencialmente

liberadora y positiva desde el punto de vista social. Continuar por el camino de falsa globalización actual generará aún más injusticias y una mayor polarización entre ricos y pobres, también dentro del primer mundo. De esta forma la globalización, lejos de globalizar a las personas, acabará por separarlas aún más. Visto así, llamar a este proceso «globalización» resulta bastante desafortunado.

7.2.1. Alejar a los ciudadanos del poder: el Consenso de Washington

La expresión «Consenso de Washington» fue acuñada en 1989,[143] sin embargo el Consenso de Washington es una doctrina político-económica surgida en la década de los ochenta y de la que la globalización no es una consecuencia, sino el vehículo para ejecutar un plan maestro cuya finalidad es crear una estructura supranacional sobre la que no tenga poder los ciudadanos, ya que a sus miembros no se les eligen mediante sufragio popular alguno.[144] Esto se debe a que estas instituciones supraestatales que organizan los Estados son las encargadas de dictar las órdenes éstos deben obedecer.

La promesa de esta doctrina es que los mercados libres serán capaces de organizarse a sí mismos y generar la

riqueza que permitirá mejorar nuestra calidad de vida. Para que los mercados sean verdaderamente libres, no debe existir la menor injerencia gubernamental y pública: deben estar controlados por manos privadas y la intervención pública de su gestión estaría reducida a su mínima expresión; ésta sería eliminada en aplicación estricta de las ideas de libre mercado de Milton Friedman

Otro de los argumentos más utilizados por los partidarios de esta doctrina es que la liberalización de los servicios y la privatización de las empresas públicas que prestaban éstos servicios, unida a la uniformidad y la uniformidad transnacional que impone el sistema político-económico que se está implantando servirá para llevar la democracia a lugares remotos. Dicen que la apertura al capitalismo que China efectuó hace unos años concluirá con una petición masiva de libertad en aquel país. La realidad es muy diferente. El monocultivo económico y cultural que se impone a escala global, lejos de llevar la democracia a los países que se incorporan a este mercado común, como China, exige un debilitamiento de nuestros derechos sociales y civiles que permita que el Fondo Monetario Internacional, la Organización Mundial del Comercio y el Banco Mundial

tengan un margen de maniobra para presionar a los países que se incorporan al mercado internacional con el fin de imponerles condiciones previas a su entrada.

La falsa promesa de llevar la democracia a otros regímenes está siendo utilizada para debilitar nuestras democracias. Esto es lo que sucede cuando decisiones importantísimas para el desarrollo de nuestras vidas son dictadas por entidades cada vez más lejanas y sobre las cuales el pueblo no tiene poder, como la Organización Mundial del Comercio, el Fondo Monetario Internacional o la Comisión Europea.

Así sucede cuando el FMI decide qué país será sancionado por no reducir el gasto público, y es así cada vez que la Comisión Europea aprueba una nueva directiva que exige regular, o liberar, sectores en todos los países miembros de la UE. A la Comisión Europea, la institución con más poder de la Unión Europea, cuyos miembros -los comisarios- desempeñan el papel de «ministros europeos» para cada ámbito, no la elige el pueblo democráticamente. Sin embargo, la Comisión Europea dicta las normas para liberalizar los mercados y tiene poder para vetar las resoluciones parlamentarias, que son las únicas votadas por

representantes elegidos democráticamente.

De hecho, la Comisión tiene tendencia a ignorar estas resoluciones cuando son contrarias a su voluntad, como en el caso de las patentes de software, cuya introducción y legitimidad ha rechazado el Parlamento en más de cinco ocasiones. Ante cada rechazo, la Comisión Europea ha reaccionado iniciando los trámites para un nuevo intento de introducción de dicha normativa. Ante cada rechazo, la Comisión Europea utiliza sus poderes autárquicos para imponer su voluntad y obligar a su cumplimiento. Esto se debe a que la Comisión es elegida de forma arbitraria y actúa con prepotencia, pues no debe rendir cuentas a nadie, sabedora de que los ciudadanos no pueden elegir a sus miembros ni mucho menos decidir su expulsión del cargo.

En un sistema democrático esas decisiones recaerían en una institución elegida por los ciudadanos. En el mundo supraestatal que nos quieren imponer, parte del juego es precisamente evitar ese acceso ciudadano a las decisiones. ¿Qué cara va a poner un agricultor griego cuando le digan que la culpa de que deba destruir su cosecha la tiene un oscuro funcionario de Bruselas cuyo nombre no conoce y

sobre el que no tiene ninguna autoridad? Pondrá la cara que pondría todo aquel al que se aparta del control de su propia vida.

En materia de privacidad, libertades y derechos de reproducción este mecanismo funciona exactamente igual. Como conseguir que los veintisiete países miembros de la UE legislen a favor del muy concentrado mercado discográfico y las gestoras de derechos de autor es una tarea ardua y no libre de obstáculos (algún gobierno podría no adoptar las medidas exigidas por miedo a perder el apoyo ciudadano y por tanto el poder), se delega en la Comisión la toma de decisiones sobre estos asuntos y la emisión de la preceptiva directiva que forzará a la transposición de las decisiones así tomadas a la legislación vigente en cada Estado, so pena de ser sancionados si no lo hacen.

Los gobiernos pueden entonces tomar decisiones impopulares y escudarse en que una institución no democrática ha dictado una norma de obligado cumplimiento. Este es el paso que culmina la teoría política descrita en el Consenso de Washington para conseguir cambiar el sistema de gobierno de forma que aleje a los ciudadanos del poder que la democracia les otorga sobre las

decisiones más importantes. Es por eso que no debería sorprendernos que las medidas de control ciudadano, el recorte de derechos o el endurecimiento de la restricción de copia sean temas de los que se encarga habitualmente la Comisión Europea. Es el sistema que hace posible que se adopten las mismas sin perjuicio alguno para nuestros gobiernos, debilitando nuestros derechos mientras el sistema se mantiene en calma.

7.3. La privacidad y la ley

El respeto a la privacidad es un problema legal, de ahí que la relación entre privacidad y ley sea estrecha y haya que examinarla siempre con atención. La legislación actual en materia de privacidad se caracteriza especialmente por la falta de leyes que regulen numerosos ámbitos y por lo poco que protege nuestra privacidad en la mayoría de las ocasiones cuando hay normativas desarrolladas. La Ley Orgánica de Protección de Datos resulta insuficiente para proteger la cantidad de información personal que día a día se puede recopilar sobre nosotros.

A este respecto, es necesario mencionar que nuestro derecho a mantener fuera del conocimiento público

cualquier faceta de nuestra vida está muy mermado. Desde las deficiencias legales y la falta de protección hasta las puertas traseras permitidas por la ley y que eximen a las fuerzas de seguridad de todos los protocolos de defensa que la ley prevé para nuestra privacidad, en casi todas las ocasiones en que examinemos cómo la ley aborda el asunto de nuestra privacidad acabaremos con una cierta sensación de desamparo.

7.3.1. La Constitución de 1978 y la privacidad

Las cartas de derechos que rigen nuestra vida reconocen el derecho a la intimidad y a preservar como privado un entorno de nuestra vida que nosotros tenemos la posibilidad de delimitar. En concreto, nuestra Constitución recoge en su artículo 18 las garantías que deben existir sobre el derecho al honor, a la intimidad y al secreto de las comunicaciones. Asimismo incluye una referencia a los límites que se impondrán al uso de la informática para evitar que viole esos derechos.

Por tanto, la privacidad es un derecho constitucional. No es algo que haya que conquistar empleando contramedidas tecnológicas, aunque éstas sean

más que necesarias debido a la laxitud de las leyes que permiten la violación de este derecho fundamental. La privacidad es una cuestión legal y es en ese terreno, el de nuestra legislación, en el que hay que defenderla.

7.3.2. Ley Orgánica de Protección de Datos

Cuando hablamos de privacidad y legislación lo primero que hay que mencionar es que en la actualidad contamos con una ley que nos protege del abuso sistemático a que son sometidos nuestros datos personales: la Ley Orgánica de Protección de Datos, más conocida como LOPD.[145]

La ley de protección de datos española es bastante restrictiva, y se podría decir que está dotada de herramientas suficientes para protegernos en aquellos ámbitos de los que se ocupa. Los principales puntos de esta ley son que, siempre que se recogen datos personales, debemos ser informados, que la cantidad de datos recogidos nunca excederá a los estrictamente necesarios y que, una vez dejen de ser necesarios (o solicitemos su eliminación), deberán ser cancelados inmediatamente.

Sin embargo, el optimismo inicial que esta situación

pudiera generarnos se esfuma cuando pensamos en ámbitos cotidianos, o que lo serán en el futuro más cercano, como la recolección de información personal gracias a chips RFID o la navegación por Internet. A menudo, en Internet seremos dirigidos a páginas web ubicadas en el extranjero, fuera del alcance de la jurisdicción de la LOPD. A menudo, la información contenida en nuestros chips RFID será leída por cualquier lector ubicado en la calle sin que se nos de la opción de eliminar esa información de cualquier registro que llegue a incluirla.

Pero no es esa la única posibilidad que encontramos de que nuestros datos vuelen libres sin que la LOPD pueda impedirlo. Incluso un servicio que se nos brindase dentro de nuestras fronteras, donde la LOPD sí es aplicable, podría también burlar la misma si contractualmente aceptamos determinados usos de nuestros datos, que podrían ser perjudiciales para nuestra privacidad. Entre las más comunes de estas actividades está la reventa de nuestra información a terceras partes.[146] Estas prácticas contractuales son muy comunes y asestan un golpe al que era, supuestamente, el punto más fuerte de esta ley.

Las limitaciones de la LOPD

Cierto es que existe una ley orgánica de protección de datos que regula el uso que terceras partes pueden hacer de nuestros datos personales, recogidos por terceras personas como parte del préstamo de un determinado servicio. Esta ley regula e impide que se cometan numerosos abusos, pero tiene muchas áreas negras en cuanto nos adentramos en un entorno tan cotidiano como es la red y nuestras actividades diarias en ella.

La LOPD nos protege mínimamente de lo que los prestadores de servicios a través de Internet pueden hacer con nuestros datos personales. O mejor dicho: nos protege bien de aquellos prestadores que operan desde España, pero no nos protege en absoluto de aquellos que operan desde el extranjero, cosa más que habitual en Internet.

Estas empresas que operan en el extranjero están fuera del alcance de la LOPD, lo que encomienda la protección de nuestra privacidad a la legislación sobre estos asuntos en los países de destino, cuya protección de datos personales podría ser mucho menos férrea que la española. Este factor entra en juego también cuando se deslocalizan determinados sectores, como los departamentos de atención

al cliente de muchas empresas. Es cada vez más habitual que estos traslados empujen a nuestras empresas a trabajar en varios países, generalmente en Iberoamérica -donde los salarios son entre 5 y 10 veces más reducidos que en España-, y trasladar hasta allí nuestros datos personales.

La LOPD prevé que, en caso de que este transporte de datos se produzca, el país receptor del centro de atención al cliente deberá tener en materia de protección de datos una legislación vigente que sea tan restrictiva o más de lo que ya es la legislación española. Sin embargo, eso no se cumple en casi ningún caso.[147]

7.3.3. La retención de datos de telecomunicaciones

El 15 de julio de 2007 el Congreso aprobó una ley para transponer a la legislación estatal la directiva europea sobre retención de datos, aprobada previamente en febrero de 2006. Esta ley entró en vigor el 7 de noviembre y obligará a los operadores a guardar la traza de las comunicaciones durante el plazo de un año.

Esta traza incluye al emisor y el receptor de la comunicación, la fecha, la hora y los dispositivos empleados.

Se retendrá esta traza en comunicaciones telefónicas y también en comunicaciones a través de Internet, donde resulta paradójico almacenar sólo la traza, pues es difícil separar el inicio de la comunicación del contenido de la misma.

La ley, tal y como fue aprobada, plantea problemas de seguridad. En palabras de Pedro Martínez, teniente fiscal del Tribunal Superior de Justicia de Madrid en aquel momento, «El control judicial de la información personal que se entrega a los Agentes Facultados (nombre que la ley da a policías y agentes del CNI) no esté en ningún momento controlada por los jueces».[148] Esta situación se ve agravada por el hecho de que el juez otorgará permiso para el acceso a los registros de nuestras comunicaciones siempre que haya indicios, que no pruebas, de culpabilidad que lo justifiquen.[149]

El gran problema es que un indicio es una vaguedad, un «creo que» oído a un agente es todo lo que el juez necesita para conceder ese acceso, sin luego tener la posibilidad de supervisar qué uso se hace de esa información privada. Evidentemente, eso es exigir demasiado poco. Permitir ese tipo de acceso a nuestra información privada a

un cuerpo policial es dotarlo de poderes excepcionales que se acercan demasiado a los que podía tener la Stasi en la República Democrática de Alemania. No sé qué sucederá en el futuro, pero sea lo que sea, no creo que permitir a un cuerpo policial ese tipo de actuaciones sea la solución a ningún problema. Más bien es posible que dé lugar a abusos, ya que esta ley les confiere demasiadas atribuciones.

7.3.4. La traza privada sin orden judicial

Entendemos como traza un rastro que se puede seguir, y entendemos como trazar el hecho mismo de seguir ese rastro. La traza privada es el rastro de nuestras comunicaciones y tenemos derecho a defenderla gracias al derecho universal a la intimidad y al secreto de las comunicaciones. Este derecho al secreto de las comunicaciones está recogido en la Constitución española de 1978.[150]

Cuando hablamos de traza sin orden judicial nos referimos a la posibilidad de violar el secreto de las comunicaciones personales siguiendo un rastro (asociado a una persona) sin necesidad de orden judicial alguna que lo justifique en función, por ejemplo, de algún tipo de

investigación criminal. Desde el año 2005, en que se aprobó esta modificación legal, un agente puede obtener la traza de nuestras comunicaciones privadas sin permiso de un juez,[151] difuminando la línea que separa nuestros derechos y libertades fundamentales en favor de un poder paramilitar excesivo (por cuanto no hay moderación judicial que impida un mal uso de esta competencia) otorgado a las fuerzas de seguridad. Las comunicaciones interceptadas incluyen la recepción y envío de todo tipo de datos electrónicos (teléfono, correo electrónico, navegación, etc.).

Con el Real Decreto aprobado en 2005, se permite el acceso a la traza pero no al contenido. Pero sucede que la traza de mis comunicaciones incluye a quién envío correos electrónicos, mensajes de texto, a quién llamo, qué páginas de Internet leo y qué hardware utilizo para comunicarme. Esta información dibuja un mapa tan preciso de mis contactos y mis relaciones, que acceder al contenido de las comunicaciones apenas podría aportar algo más.

Todas estas medidas se justifican en nombre de la seguridad, pero ¿de qué seguridad están hablando? La seguridad de la que hablan no es la que parece: no pretenden defendernos de un peligro mayor, como pudiera

ser el terrorismo, quieren defender al Estado de sus propios ciudadanos. La posibilidad de prever delitos a raíz de estos análisis es mínima. Sin embargo, es posible elegir una persona a la que se quiere investigar y de la que se quiere conocer su vida. La diferencia es que esto último ya se podía hacer sin necesidad de este Real Decreto, y se limitaba el seguimiento y el espionaje de comunicaciones privadas a aquellos casos relacionados con crímenes en los que el juez accediera a permitirlo. Ahora lo hemos masificado, y eso no puede ser bueno.

La imposibilidad teórica de realizar la traza electrónica es simplemente legal y viene dictada por el derecho al secreto de nuestras comunicaciones que recoge nuestra Constitución, pero también en el derecho, asimismo recogido por la Constitución, de que se limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de nuestros derechos.[152]

Quizá como dijo Thomas Jefferson, «puede que llegue el día en el que, no aspirando más que a sentimientos de amor a nuestro país, su libertad y su felicidad, nuestra correspondencia deba ser tan secreta como si

maquinásemos su destrucción». Comparto el final de esta frase: nada hace más seguro a un país que la seguridad de sus ciudadanos, y ésta está basada y recibe todo su impulso de limitar el control y el poder que los Estados tienen sobre ellos.

7.3.5. Las bases de datos

Una de las características de la informática, que nace del mismo corazón del diseño de las computadoras y de sus capacidades, es la ingente cantidad de datos que es capaz de manejar en un tiempo muy pequeño. La forma en que estos datos se acumulan y clasifican para que su acceso sea óptimo en términos de tiempo necesitado para la consulta e información obtenida es lo que llamamos base de datos.

Si algo caracteriza el momento que vivimos actualmente es la ingente cantidad de bases de datos, y el creciente tamaño de éstas, que día a día se crean y que cada vez almacenan más información. Estas bases de datos pueden tener titularidad pública o privada.

Bases de datos públicas

Es cada vez más frecuente que los gobiernos

construyan enormes bases de datos con información personal de sus ciudadanos. Esta información puede abarcar desde lo más elemental (nombre, domicilio, etc.) hasta información de carácter bastante diverso (historial médico, de pago de impuestos, antecedentes penales, filiaciones políticas, número de teléfono, dirección de correo electrónico, etc.). Éstas, lejos de haber tocado techo, están en auge y pronto recogerán todo tipo de información, ya que parece que la Comisión Europea considera estratégico para nuestra seguridad conocer la vida sexual de los ciudadanos europeos.[153]

Sin embargo, las bases de datos que se han multiplicado con la era digital no son algo nuevo: en España se recoge incluso la información referente a las reservas de hoteles, y en toda la Unión Europea existe una tendencia alarmante a la construcción acelerada de bases de datos con información biométrica, generalmente ADN, huellas dactilares e iris. Desde la entrada en vigor de la ley que obliga a la retención de datos de telecomunicaciones, también la traza de estas comunicaciones engrosa las bases de datos con información sobre los ciudadanos que controlan los gobiernos.

En su conjunto, la cantidad de información que los gobiernos actuales tienen sobre sus ciudadanos excede, con mucho, la que los regímenes más sangrientos de la historia hubieran soñado poseer. Esta tendencia no deja de agravarse debido a que en la mayoría de los casos estas bases de datos se confeccionan recogiendo mucha más información de la necesaria, ignorando el principio de proporcionalidad y el carácter mínimamente lesivo que exige la LOPD. Como quiera que los protocolos de seguridad a la hora de acceder y permitir el acceso controlado a esta información no garantizan (en última instancia, no se pueden garantizar en ningún caso) la ausencia de abusos, es importante exigir a muy corto plazo una reducción de la información personal que es almacenada y controlada por los Estados.

Se estima que en Reino Unido hay unas cuatro millones de personas «fichadas» en la masiva base de datos de ADN. Los representantes de minorías étnicas han denunciado que la mayoría de los individuos vigilados pertenecen a estas minorías: un 77 % de los negros británicos o residentes en Reino Unido tienen su ADN incluido en este fichero.[154] El número de personas incluidas en esta base de datos aumenta al ritmo estimado de unas

cincuenta mil personas al mes y se ha denunciado que, aunque se demuestre la inocencia del individuo, éste no tiene posibilidad de eliminar sus datos de esa lista que supuestamente está destinada a sospechosos y culpables.[155] Este modelo ha sido exportado a otros países como Francia o España, donde una base de datos con información biométrica similar comenzó a funcionar en noviembre de 2007.[156]

Ya se han cometido abusos con estas bases de datos públicas, como las detenciones previas a la reunión de alto nivel que se celebró en Canadá para negociar la ampliación del Tratado de Libre Comercio para Norte América (*TLCAN*, o *NAFTA*, por sus siglas del inglés, *North America Free Trade Agreement*) más allá de México hasta incluir 34 países de América Central y del Sur. Los días previos a esta reunión, conocidos activistas estadounidenses que pretendían acudir a Canadá para manifestarse pacíficamente y pedir un tratado de comercio más justo con los países pobres, fueron encarcelados sin cargos. Los activistas fueron liberados después de que la reunión se hubiera celebrado, cuando su participación ya no era importante para la organización de los grupos de protestas.[157] ¿Qué tenían que temer los

gobiernos de Canadá y Estados Unidos de estos activistas pacifistas? No lo sabemos, pero cuando un país supuestamente democrático demuestra con hechos que conocer demasiado sobre las personas puede llevar al abuso de poder, el debate sobre la legitimidad de la información que el Estado acumula sobre las personas debería incluirse en la agenda pública y la cantidad de información que el gobierno acumula sobre las personas debería limitarse sustancialmente de forma legal.

Bases de datos privadas

La gran mayoría de las bases de datos existentes son de titularidad privada. Quizá no son las más comprometedoras, pero alguien con acceso a varias de estas bases de datos, o con capacidad para hacer minado de las mismas y relacionar la información de éstas, podría configurar un mapa bastante preciso acerca de nosotros: nuestros gustos, nuestras aficiones, nuestros contactos y actividad cotidiana, nuestras compras. La empresa que controla la base de datos podría incluso delatarnos ante un Estado supuestamente democrático que pretenda censurarnos aun cuando no exista una orden judicial que lo justifique, como fue el caso de Google y el Estado de Israel.[158]

De ahí que estas bases de datos privadas sean también muy importantes.

El mayor problema que plantean estas bases de datos es que por lo general los acuerdos de prestación de servicios incluyen cláusulas en las que cedemos estos datos y permitimos usos que de otra forma no serían posibles conforme a la protección que brinda la Ley Orgánica de Protección de Datos. De esta forma, nos encontramos con que uno de los pocos ámbitos problemáticos para nuestra privacidad sobre los que se ha legislado de forma efectiva se ve completamente subvertido por las condiciones de uso que aceptamos en muchos contratos.

Por supuesto, al ser una cláusula contractual nos compete a nosotros renegociarla. El problema surge cuando todos los prestadores de servicios incluyen este tipo de cesiones en los contratos, ya que todos esperan hacer negocio con nuestros datos. Ante esto no quedaría más que rechazar todos los contratos y forzar un cambio de actitud de éstos. El problema es que nuestra información personal posee un valor mayor de que se le atribuye habitualmente, por eso no juzgamos adecuadamente la necesidad de realizar movilizaciones que nos ayuden a protegerla. Por este mismo

motivo, pocas personas se negarán a firmar contratos que incluyan este tipo de subversiones de nuestra privacidad.

¿A quién pertenecen estas bases de datos?

Cuando se plantea esta pregunta, se parte de la base de que la legislación actual plantea la titularidad de estas bases de datos como propiedad de la empresa, siempre dejando en manos de los usuarios el ser excluidos de los ficheros a voluntad, así como obligando a la empresa a rescindir la información de las personas una vez que el contrato que llevó a la inclusión deja de tener vigencia.

Pero más allá de la situación actual de la ley, ¿es posible considerar que la titularidad de las bases de datos donde se almacena información privada, que va desde la información personal básica hasta sus usos y el rastro de navegación, las llamadas, el consumo y prácticamente todos los ámbitos de nuestra vida, es propiedad de una empresa?

En el fondo, el problema de las bases de datos es el mismo tipo de problema que atañe a la comunidad académica con la aparición de Open Access, iniciativa que defiende el libre acceso a los resultados de las investigaciones sufragadas con dinero público y a la que

poco a poco se van adhiriendo los Estados. Es importante encontrar la manera de que los datos recuperen el valor que tienen para nosotros, sin que este valor sea eclipsado por el rendimiento económico que los mismos puedan ofrecer a un sector empresarial. Es exactamente el mismo tipo de cambio que se produce entre la industria editorial científica y las publicaciones Open Access. Resulta primordial reenfocar el modo en que se relacionan las personas, que tienen una tendencia innata a compartir, con las empresas de Internet que ofrecen el servicio y que, de esta forma, adquieren el control sobre los datos. La reforma debe hacer posible que los datos sigan siendo propiedad de las personas. No se exige la posibilidad de acceder, modificar o eliminar los datos. Se exige la titularidad de los datos (texto, imágenes, vídeo, datos personales), que son cedidos a la compañía en el marco de una prestación de servicio y que serán devueltos tan pronto se ponga fin a ese acuerdo. Open Access comienza ya a crear tensiones en un sector importante como el editorial científico, que pronto deberá estructurar su especulativo modelo conforme a otro sistema. ¿Por qué no se va a poder aplicar en otros ámbitos?

Por supuesto, la recogida de toda esta información

personal está contemplada en la mayoría de contratos de prestación de servicio actuales, pero ¿hasta qué punto es posible regular cómo se va a usar esta información o si, hasta cierto punto, la titularidad de las bases de datos pertenece a los usuarios, aunque temporalmente cedan los datos a la empresa? La lucha por regular el uso y abuso que se hace de las bases de datos, así como la información personal que se pueda incluir en ficheros de este tipo, es la batalla más importante que tenemos que librar ahora mismo. Va a ser especialmente dura, y no podemos anticipar, ni con mucho, un éxito como el cosechado por la comunidad del software libre, ya que para conseguir esta victoria será importante crear primero una comunidad con conciencia de la necesidad de defender estos datos personales. Esa comunidad, aunque incipiente, está aún en una fase muy temprana de su desarrollo e impulsarla es una de los retos más importantes que tenemos por delante.

La ingeniería social y nuestros datos

Cuando hablamos de ingeniería social nos referimos a la capacidad de conseguir información privada de alguien mediante el uso de técnicas de subterfugio. De esta forma conseguimos información de forma legítima sin tener que

violar la legislación y sin necesidad de realizar complejos ataques informáticos.

El mecanismo por el que funciona la ingeniería social es de una simplicidad sólo comparable a lo extendido de su aplicación. Un ejemplo: cuando nos inunda una avalancha de tecnicismos legales a la hora de contratar un nuevo servicio (telefonía, gas, etc.) y subyugados por semejante ladrillo legal decidimos no leer hasta al final pero firmar en cualquier caso. Simple ingeniería social.

Evidentemente, la única posibilidad de evitar este comportamiento sería legislar de forma que no fuera permitida la cesión por vía contractual de información privada para determinados usos. Esa posibilidad es conflictiva y poco probable. Por tanto, la única la única manera de deshacernos de este problema es educarnos a nosotros mismos para leer los contratos que firmamos y no aceptar usos que consideremos abusivos siempre que sea posible.

La mayoría de los contratos de prestación de servicios están diseñados por los propios prestadores que, ante la reducida competencia existente en muchos ámbitos, seguramente acabarán imponiendo una puerta trasera para

colarse por entre las vallas que la LOPD levanta para proteger nuestra privacidad.

El caballo de Troya de la LOPD

El tercer gran problema de la LOPD es que no pone límites a la información que el Estado puede pedir sobre los ciudadanos. El artículo 6 de la actual LOPD exige el consentimiento inequívoco de la persona, excepto en el caso de las Administraciones Públicas, que recogerán cuanta información necesiten para el correcto desempeño de sus funciones sin necesidad de informar al ciudadano.

Este punto hace posible que toda información que nosotros otorgamos a un prestador de servicio sea interceptada en cualquier momento por la administración pública. Si todo lo anterior no nos hubiera hecho reflexionar, aquí tenemos un motivo más que suficiente para hacerlo: al cúmulo de información personal que el estado ya reúne sobre nosotros hay que añadir que toda información controlada por una entidad privada puede acabar también en manos del Estado sin que medie control judicial y se nos informe de ello.

7.4. Legislación y RFID

Además de las limitaciones prácticas que la LOPD encuentra cuando nos desenvolvemos en la red, existe otro ámbito en el que la Ley Orgánica de Protección de Datos no ofrece garantías ni seguridad y donde su aplicación resulta absolutamente ineficaz. Este ámbito está representado por la tecnología RFID, que permite recopilar una ingente cantidad de datos sobre las personas y cuyo uso carece completamente de regulación en España. En otras palabras, la LOPD no dice en ningún momento cómo pueden utilizarse los datos recogidos utilizando tecnología RFID, que pueden vincularse con facilidad a la identidad de la persona. La LOPD no dice dónde no podrá recogerse información personal utilizando estos chips.

Lo único que se ha regulado a este respecto son las frecuencias que serán reservadas para diferentes aplicaciones. Esta regulación no está relacionada en forma alguna con la defensa de nuestra privacidad, sino que más bien tiene que ver con el trabajo previo de organización que facilitará la llegada del elefante empresarial a este sector.

Otro gran problema es que la LOPD asegura unas sanciones para aquellos que violen las condiciones legales

que su texto impone, pero a menudo la cuantía de estas sanciones es mucho menor que el beneficio obtenido de comerciar con nuestros datos. Ello supone *de facto* que las sanciones previstas no pongan freno a la violación de la ley, pues la cantidad de dinero que se puede ganar es siempre muy superior a la sanción que acarreará dicha actividad negligente.

7.4.1. La ley ideal sobre RFID

La legislación sobre RFID es prácticamente inexistente y lo más parecido que encontramos es una regulación del espectro de radiofrecuencias para diferentes usos. No hay nada regulado en materia de privacidad y si algo deducimos de ese vacío legal es que necesitamos leyes que regulen el uso de la tecnología RFID.

La ley ideal sobre RFID debería tratar al menos dos puntos, que harían de eje y sobre los que se podrían matizar los detalles si estos dos puntos conservaran su espíritu: los chips RFID deben ser absolutamente opcionales, ningún producto los debe traer integrados por obligación y éstos nunca deben estar presentes en la documentación oficial.

Todo chip RFID se nos fuera entregado mediante un

sistema de *OPT-IN*. La inclusión de un chip RFID en cualquiera de los objetos que compramos debe ser opcional. Eso significa que los aceptamos sólo si queremos y que en ningún caso nos pueden obligar. La opción por defecto debería ser que los objetos no incluyan estos chips, de forma que si estamos interesados en participar en los sistemas de mercadotecnia y seguimiento solicitemos su inclusión/añadido o una versión del producto que lo tenga implantado. Esto sería válido para tarjetas (crédito, abono de transporte, fidelidad) y objetos de todo tipo (neveras, sellos de correos, zapatos, revistas) excepto para la documentación oficial.

Además, todo objeto que incluya un chip RFID debe estar correcta y visiblemente etiquetado indicando este hecho, que debe constar de forma clara. Los chips deben poder ser neutralizados y ser retirados de los objetos sin que tenga repercusiones en la garantía de los mismos. Esto puede ser incompatible con el implante de RFID en origen (*source tagging*), pero es que este implante en origen está en contra del sistema OPT-IN propuesto, por lo que no debería ser un problema añadido.

Ninguna tarjeta de identificación oficial debe incluir

chips RFID. Sin opción. Los chips RFID son inseguros y violan nuestra privacidad. La inclusión de estos chips en documentos oficiales es contraproducente. Los documentos que actualmente no los incluyen no deberían incluirlos en el futuro y para ello se deberían realizar las reformas legales necesarias. Esto último es realmente urgente: hay que eliminar los chips RFID de los pasaportes, así como evitar que se introduzcan en otros documentos oficiales.

Debe protegerse y garantizarse la disponibilidad de medios y herramientas para que podamos permitir y bloquear la emisión de estos chips a voluntad. Estos dispositivos suelen emplear el mecanismo de la jaula de Faraday para aislar un objeto con uno de estos chips: es imprescindible defender la legalidad de estos dispositivos protectores (por ejemplo, fundas anti-RFID) como parte vital del sistema que debe devolver a las personas el control de su privacidad.

7.5. Legislación y videovigilancia

La instalación de videocámaras y el tratamiento de los datos obtenidos mediante éstas se encuentran regulados dependiendo de si la videovigilancia la llevan a cabo por

instituciones públicas o privadas.

Esta legislación debería garantizar el perfecto desarrollo de nuestros derechos constitucionales. Sin embargo, desde muchos puntos de vista es la instalación misma de las videocámaras, y no su ausencia, la que impide el perfecto respeto de muchos de nuestros derechos básicos, como el derecho a la intimidad personal y familiar y el derecho al honor.

7.5.1. Videovigilancia pública

Estos derechos constitucionales se han visto pisoteados desde la redacción misma de la ley que regula la videovigilancia por parte de las fuerzas de seguridad públicas,[159] que considera que "las imágenes y sonidos captados, reproducidos y tratados mediante estos sistemas no serán considerados intromisiones ilegítimas en el derecho al honor, la intimidad personal, familiar ni el derecho a la imagen".

Evidentemente, la necesidad de definir esta puerta trasera desde el segundo artículo de la ley en vigor nace de la evidencia factual de que se están produciendo estas violaciones, pues mi intimidad no es adaptable y no varía de

tamaño ni de forma dependiendo de quién me esté grabando. ¿O acaso el principio de proporcionalidad predicado en la misma legislación no exige, copiando literalmente el texto legal, "la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas"?[160] Este mismo artículo entiende como principio de proporcionalidad el instalar las cámaras allí donde sea realmente necesario para salvaguardar la seguridad de las personas y de los bienes inmuebles, pero esta proporcionalidad no se aplica a las grabaciones de las fuerzas de seguridad.

Sin duda, el hecho de que la propia ley contemple la posibilidad de que las fuerzas del Estado no se rijan por las más básicas reglas de nuestra Constitución es algo que debería eliminarse en una futura revisión de la ley, en favor de una mayor transparencia y en favor también de inspirar más confianza ciudadana en nuestras instituciones y poderes públicos, ya que ahora existe una falta de comprensión social de esta respuesta desproporcionadamente coercitiva.

7.5.2. Videovigilancia privada

La videovigilancia privada está regulada a través de una instrucción publicada en el BOE en el año 2006 y Instrucción 1/2006 de 8 de noviembre de 2006, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras[161] y el comentario que la AEPD hace al respecto de ésta.[162]

Las entidades privadas que instalen videocámaras no tendrán tanto poder como las instituciones públicas. La normativa en vigor prevé que la instalación de videocámaras tenga lugar sólo cuando no sea asumible, por coste o por dificultad, vigilar un espacio mediante otro sistema. Las zonas videovigiladas deberán estar debidamente señalizadas («ZONA VIDEOVIGILADA») con una nota que incluya información de contacto sobre el responsable de las grabaciones, por si fuera necesario comunicarse con él porque se considera invadida nuestra intimidad. Las grabaciones no podrán nunca recoger imágenes de zonas públicas y estarán sometidas a la LOPD.

El principal problema es que el requisito de instalación implica la instalación por parte de una entidad

autorizada y la certificación de que el sistema está funcionando conforme a la Ley Orgánica de Protección de Datos. ¿Por qué es esto un problema? Porque la dificultad de verificar que esta protección se está realizando realmente es alta y su verificación excede con mucho la instalación misma del sistema de videovigilancia para incluir también el modo en que se registran, almacenan y custodian estas grabaciones. Sin embargo, eso no detiene a los certificadores a la hora de validar las nuevas instalaciones (y hacer caja con ello), aunque existan motivos para pensar que si la Agencia Española de Protección de Datos (AEPD) revisara estas instalaciones, encontraría no pocas irregularidades.

Uno de los principales puntos débiles de esta normativa es precisamente este último aspecto que acabamos de comentar: cualquiera puede instalar su propio sistema de videovigilancia con la única condición de que se informe a la AEPD. Como las instancias oficiales están convencidas de que cualquier espacio está mejor vigilado con una cámara, justificar la pertinencia de su instalación parece tarea harto sencilla. Esto ha posibilitado el crecimiento del parque de videocámaras instaladas por todas partes: desde panaderías hasta aparcamientos

privados, desde pequeñas tiendas de ropa hasta enormes almacenes. Todos quieren tener su cámara. Todos quieren contribuir al panóptico, al «vigilar y castigar» de que hablaba Foucault.

Sin duda, la regulación de la videovigilancia necesita una revisión importante si queremos que nuestro derecho a la intimidad sea salvaguardado.

7.6. Legislación sobre propiedad intelectual

Éste es sin duda uno de los ámbitos de la legislación que más trascendencia tienen en el ámbito público, pues los poderosos sectores empresariales que dependen de la restricción de copia para hacer viable su modelo de negocio han presionado para que se incluyan estos asuntos en la agenda pública.

Las resoluciones que se adoptan en lo referente a la legislación sobre propiedad intelectual e impulso de una sociedad digital verdaderamente libre tienen importantes consecuencias en nuestros derechos y, si bien en la mayoría de los casos no va a afectar directamente a nuestra privacidad, afectan a otros derechos básicos. Se dan también

situaciones en los que se viola nuestra privacidad para defender la propiedad intelectual, como es el caso de la intercepción de la conexión a Internet en busca de personas que comparten archivos en las redes p2p.

En materia de propiedad intelectual, la doctrina continental pone, frente a la doctrina estadounidense, un mayor énfasis en la defensa del creador, en lugar de en la defensa del mecenas. Es por ello que actos lícitos como la copia privada para uso personal han sido tradicionalmente permitidos en Europa, frente a la tajante prohibición norteamericana.

7.6.1. El Consenso de Washington en la propiedad intelectual

Sin embargo, esta tendencia está cambiando desde principios de la década de los noventa, cuando el Consenso de Washington se materializó y, en este campo, promulgó la armonización de la legislación en materia de propiedad intelectual en tantos países del mundo como fuera posible, asunto en el que Estados Unidos se ha mostrado especialmente agresivo. La estrategia escogida es presionar a terceros países, africanos o asiáticos, para que aprueben durísimas medidas en materia de propiedad intelectual a fin

de poder continuar con la presión en Occidente con la excusa de la *armonización legislativa* en el ámbito internacional. El principal interés de Estados Unidos en este asunto reside en que tan sólo durante 1998 obtuvo un balance neto superior a los veintitrés mil millones de dólares de beneficios en exportaciones de bienes relacionados con la industria de la propiedad intelectual.[163]

Así, Estados Unidos ha negociado el endurecimiento progresivo de esta legislación en diferentes países poniendo sobre la mesa condiciones muy estrictas, como expulsar -o no permitir el ingreso- a algunos países de las instituciones internacionales (como la Organización Mundial del Comercio) o la denegación de créditos (del Fondo Monetario Internacional) a aquellos países que se negasen a endurecer su LPI.[164] El fin último es eliminar toda posibilidad de que la poderosa industria norteamericana del *copyright* vea su negocio mermado por la existencia de lo que sería un equivalente de los «paraísos fiscales» en materia de propiedad intelectual.

El monocultivo cultural impuesto desde el nuevo continente viene apoyado en la restricción de copia necesaria para preservar una industria que flaquea ante las

nuevas posibilidades que plantea Internet y la negación perpetua que ella misma ha mantenido de esta realidad, negación que la ha incapacitado para plantear alternativas de negocio efectivas.

7.6.2. La Ley de Propiedad Intelectual. LPI

La última reforma de la Ley de Propiedad Intelectual fue aprobada en el Congreso en 2006 con el voto a favor de todos los partidos políticos del arco parlamentario, y sus mayores consecuencias fueron la reducción de la posibilidad de realizar copias privadas, aún permitidas pero cuyo ámbito ha pasado a estar amparado por «lo privado» para estar amparado por «el origen legal» de la obra que estamos copiando. Es un pequeño matiz mucho más importante de lo que parece a simple vista, ya que el origen legal es algo mutable en próximas reformas, mientras que el ámbito privado siempre será el ámbito privado. Aunque se especuló con la limitación a tres del número de copias privadas permitidas de una obra original, afortunadamente este punto fue eliminado del texto final. Una gran alegría, ya que este punto habría legalizado *de facto* la inclusión de sistemas de gestión digital de restricciones en todas las obras.

Otro detalle importante de esta LPI es que por una parte obliga a la industria a ofrecer las herramientas necesarias para permitir la copia privada de las obras, a la par que prohíbe la eliminación de todo sistema anticopia. Parece evidente que en caso de que la industria cumpliera con su obligación legal, no harían falta utilizar técnicas de evitación de sistemas anticopia. La realidad es bien diferente: la industria no va a facilitar estas herramientas, pues eso haría que todas las restricciones de copia que ha obtenido en numerosos países se pudieran ver fácilmente eliminadas. Así, la industria está obligada a facilitar unas herramientas que no facilitará, pero nosotros tenemos prohibido desbloquear los contenidos por nuestra cuenta.

Para finalizar, aunque el canon ya existía en anteriores versiones de la Ley de Propiedad Intelectual, fue esta reforma de 2006 la última en aumentar su cuantía y la que extendió su aplicación a todo tipo de «dispositivos idóneos para almacenar datos». Este tributo asciende a una cifra en torno a cien millones de euros anuales, que son recaudados y gestionados por entidades privadas de gestión de derechos de autor.

7.6.3. La Ley de Medidas para el Impulso de la Sociedad de la Información. LISI.

La ley de Medidas para el Impulso de la Sociedad de la Información, aprobada durante el gobierno de Rodríguez Zapatero estaba destinada a sustituir a la Ley para la Seguridad de los Servicios de Internet (LSSI) desarrollada durante el gobierno de Aznar, y que en su día ya provocó acalorados debates y protestas entre los activistas y los colectivos más involucrados en la defensa de las libertades en el contexto digital.

La LSSI fue aprobada en 2002 y desde su nacimiento contó con la oposición mayúscula de los movimientos activistas del software libre y la cultura libre. En aquel momento la entonces oposición decía oponerse a esta reforma y prometía eliminarla tan pronto como accediera al poder. Una vez más, la realidad fue bastante diferente y, ya en el poder, Rodríguez Zapatero no sólo no derogó la LSSI, sino que la reformó y endureció mediante la LISI.

Entre los puntos más polémicos y dañinos de la LISI destacaremos la posibilidad abierta a la censura mediante la inclusión de un artículo que prevé el cierre de páginas web por una autoridad competente no judicial.

7.6.4. La ruptura con las fuerzas políticas

En los últimos años hemos visto la llegada de un nuevo orden mundial, un orden que no se entiende como una nueva alineación y equilibrio de fuerzas entre las distintas potencias mundiales, aunque este reequilibrio pueda haberse producido, sino como el advenimiento de una nueva forma de organización social que es posible gracias a las tecnologías digitales y a la sociedad en red, permanentemente conectada.

Como parte de esta migración hacia la sociedad digital, ha tomado cuerpo una nueva manera de entender la estructura de poder y la toma de decisiones, si bien las viejas estructuras, encarnadas en gran medida en los partidos políticos, no están sabiendo ver a tiempo estos cambios y se aferran con todas sus fuerzas a su modelo cerrado. Como parte de la estrategia para mantener su estructura de toma de decisiones, necesitada en todo momento de un nodo que ordene y filtre, los Estados y los grandes oligopolios económicos ven en la limitación de las libertades en la red uno de los puntos cruciales de su lucha: la recuperación del poder para controlar qué puede circular, quién puede hacerlo circular y cuándo.

Pero la gran masa social que elige a sus representantes, supuestamente dedicados a servirlos con eficiencia, no quiere ver limitadas sus libertades, ni la libertad de copia de información ni la libertad de expresión, y se ha opuesto con mucha fuerza a todas las leyes que en los últimos años se han desarrollado para regular la red. Campañas como "Todos contra el canon"[165] han reunido más de dos millones de firmas ciudadanas y, a pesar de ello, las fuerzas políticas han hecho oídos sordos a las peticiones y la voluntad popular.

Desde la LSSI a la LPI, pasando por la traza privada sin orden judicial y la retención de datos de las telecomunicaciones, hasta llegar inevitablemente a la LISI, el pueblo ha visto una y otra vez que aquellos a los que había elegido para que la hicieran valer su voluntad, la han despreciado. Esta violación de la voluntad de aquellos a quienes los partidos dicen representar proviene sin duda de la necesidad de fortalecer legalmente una forma de gobierno que les otorga un férreo control del poder justo cuando más y más gente comprende que en la sociedad digital son posibles otras formas de organización, más participativas, más libres y menos sujetas a decisiones unilaterales de unos

dirigentes que tienden a velar demasiado por sus propios intereses.

El hecho de que los beneficiados al tomar decisiones de control sobre la red no sean unos partidos políticos frente a otros, sino los partidos políticos frente al resto de la sociedad hace posible perversiones políticas como que todo el espectro político esté de acuerdo en aprobar estas leyes; y cuando existen disensiones, éstas ocurren porque determinados partidos querrían endurecer aún más las medidas o porque se acerca la campaña electoral y alguien está mintiendo para embaucar a un electorado descontento. La consecuencia es que cada vez más personas están en completo desacuerdo con la práctica totalidad de las fuerzas políticas representadas en las cámaras legislativas, lo que da lugar una pérdida de fe creciente en las mismas y la desaparición de toda credibilidad que pudiera haber en las medidas que emanan de ellas.

Nuevos tiempos demandan nuevas formas de entender y hacer la política. Si los partidos crecieron al amparo de las comunicaciones telefónicas y del telégrafo, las nuevas conexiones digitales deben evolucionar hacia una nueva forma de hacer política que impida que la voluntad

popular sea ignorada. Para ello es indispensable que la red siga siendo libre y distribuida, neutral y participativa. Para ello es indispensable defender la libertad de la red ahora, pues está amenazada.

Un porqué

El motivo oficial que dicen esgrimir cuando se solicita un mayor control de la red puede ir desde el argumento habitual de la protección de una industria amenazada hasta la seguridad nacional. El problema es que, en caso de que hubiera que proteger a una industria amenazada (que tengo mis dudas de que éste sea realmente el caso), esta ayuda debería ser gestionada por una institución pública que velase por la transparencia de la gestión, cosa que no sucede. Y asumir eso sería asumir que hay que apoyar a estos sectores, pero no recuerdo que los fabricantes de congeladores pagaran un canon a los vendedores de hielo y de sal, conservantes por excelencia hasta la llegada del motor de Carnot inverso. Si un modelo de negocio deja de funcionar, la solución no es moldear el mundo, sino cambiar de negocio.

Muchos dicen ver en la libre interconexión de las

redes un tránsito inagotable de obras protegidas. Donde ellos ven un agujero por el que su bolsillo no para de perder dinero, muchos otros vemos difusión cultural, libertad de expresión y cultura compartida. Donde ellos esgrimen una defensa de la propiedad intelectual, muchos vemos zarandeada nuestra libertad de expresión y un peligro creciente para la neutralidad de la red, el único factor que garantiza la libertad de expresión en la sociedad digital. Donde ellos argumentan que se trata un simple control para evitar la violación de los derechos de autor, un sector creciente de la sociedad teme que nuestra identidad y nuestros datos sean seguidos a través de la red para ser utilizados en nuestra contra. Y allá donde no quieren que miremos, nosotros alcanzamos a ver una sociedad bajo control, violación de nuestra privacidad y supresión de nuestros derechos básicos.

7.7. El voto electrónico

Se denomina voto electrónico a todo un conjunto de sistemas cuyo punto en común es que pretenden sustituir el sistema electoral tradicional (con urnas y papeletas) por otros sistemas de votación y recuento, generalmente empleando una computadora y software diseñado a tal

efecto. Estas máquinas podrán emitir o no un justificante del voto.

La primera pregunta que todos deberíamos hacernos cuando evaluamos la posibilidad de aceptar el voto electrónico es en qué serviría para mejorar el sistema de votación convencional y qué debilidades tiene. No existe en la actualidad un sistema de voto electrónico que aguante la comparación con el sistema tradicional que todos conocemos.

Si hablamos de fiabilidad de los resultados, este factor por sí mismo ya sería suficiente para que nos convenciésemos de la necesidad de rechazar todo sistema de voto electrónico. Manipular unas elecciones en las que se emplee el voto tradicional es complicado. Requiere gente involucrada en muchos lugares diferentes, pues una sola urna amañada no dará un vuelco al resultado final, y es difícil que le pase inadvertido a facciones políticas rivales que casi con toda seguridad mantendrán observadores en la mayoría de mesas electorales para velar por un recuento limpio de los votos. De esta forma, el voto tradicional es un voto que difícilmente puede ser manipulado sin que la oposición política y la opinión pública se percaten de ello.

Unos cientos de observadores distribuidos por el país de turno suelen ser suficientes para velar por la limpieza de las elecciones.

Con el sistema de voto electrónico la situación es radicalmente diferente. Al no haber recuento de papeletas y no existir tampoco en muchos casos una papeleta con el registro del voto (ni la exigencia legal de que esta papeleta exista), aumenta la posibilidad de que un número pequeño de personas (que por tanto serán más difícilmente detectables) manipule el resultado sin ser descubiertas.

Adicionalmente, una de las paradojas de la democracia es que para el pleno ejercicio de una democracia que defiende nuestras libertades el voto debe ser secreto. Y lo es precisamente para evitar males mayores allí donde nuestra libertad se supone defendida por el sistema. Uno de los problemas del voto electrónico es que existe trazabilidad del voto. En las votaciones convencionales es imposible averiguar qué sobre pertenece a cada votante, pero en el caso del voto electrónico bastará un control del orden en que cada ciudadano votó en cada máquina para poder trazar, mediante los resultados almacenados por el software que lleva a cabo el recuento, qué ha votado cada persona. No

conviene olvidar que la Declaración Universal de los Derechos Humanos reconoce como derecho básico la posibilidad de emitir el voto en secreto y mediante un mecanismo que garantice que es emitido en total libertad.[166]

Todos estos problemas se ven agravados si las máquinas de voto electrónico no emplean software libre, característica generalizada en todas ellas, ya que cuando no se tiene acceso al código del software, no se puede saber con exactitud si el software miente o no a la hora de realizar el recuento de votos. En este sentido es interesante señalar que informes emitidos por entidades independientes contratadas por el gobierno de Reino Unido consideran que no sólo el voto electrónico es ilegal, sino también otras modalidades, como el voto por Internet e incluso el voto postal, pues ninguna de estas formas de votación garantiza que se cumpla lo que dicta la Declaración Universal de los Derechos Humanos en lo referente al secreto y, sobre todo, en lo referente a la libertad de voto: ni el voto postal ni el voto por Internet garantizan que mi voto esté libre de presiones externas que lo dirijan; del mismo modo que también la pérdida del carácter secreto del mismo afecta a la independencia con la que tomamos nuestra decisión de

votar.[167]

Por todo lo anterior, el voto electrónico es indeseable e incompatible con una sociedad democrática, ya que la salud y la limpieza de nuestra democracia se verían seriamente socavadas con la introducción de estos sistemas de votación.

7.8. Conclusiones sobre legislación y privacidad

Recordemos una vez más que la defensa de la privacidad no es un problema tecnológico, sino un problema legal. No es que el abaratamiento de la tecnología haga posible ciertos sueños represivos, sino que la ley no regula adecuadamente los usos de algunas tecnologías que están inundándolo todo.

Desde la laxitud de las normas que regulan la videovigilancia hasta el fin del secreto de las comunicaciones, la traza privada sin control judicial, la retención de datos y el más absoluto páramo sin regular que rodea a la RFID, las normas para proteger nuestra privacidad brillan por su ausencia. ¿Dónde queda ese pequeño detalle constitucional que reza que se limitará el uso de la

informática para impedir que un uso desmedido ponga en peligro nuestros derechos a la intimidad personal y familiar? Hasta donde puede observarse, no existe un mecanismo legal eficaz que limite el uso de la tecnología y la informática para invadir nuestra privacidad.

Por eso si existe alguna conclusión sobre todo este asunto es precisamente que necesitamos leyes, más y mejores, que nos ayuden a prevenir los abusos que en nombre de nuestra seguridad y de la guerra contra el terror se perpetran contra nuestra privacidad, ya muy maltrecha.

El sentido en que fluye la información define la estructura de poder y, por ese motivo, todo poder aspira siempre a obtener más información. Los gobiernos siempre han mantenido sistemas de espionaje que han empleado para saber qué se planeaba tanto fuera como dentro de sus fronteras, para vigilar a otros Estados pero también para vigilar a ciudadanos que tenían ideas diferentes. Los gobiernos tienen poder, aun en un Estado débil como el actual, y su instinto les pide más poder para perpetuarse. En democracia, el deber de la ciudadanía y de la justicia es precisamente refrenar los deseos de más poder de los poderes político y económico, ya que a menudo no se dudará

en espiar masivamente a la población para que para prever y evitar con una respuesta calculada cualquier acción, por justificada que esté, por parte de aquellos que nos controlan.

Necesitamos movilizarnos para aportar algo de mesura a la desmedida política de seguridad actual, basada en el control de los ciudadanos. Necesitamos detener el avance de la sociedad de control que nos están fabricando, mantenernos a este lado de la puerta hasta que se nos garanticen nuestros derechos básicos, de forma que la sociedad digital no se convierta en el sumidero de todos los derechos civiles que otros lucharon por conseguir.

8. ¡Acción!

Introducir un capítulo como éste en el tramo final de un manual como el que están acabando de leer me parece un gran atrevimiento, pero creo que puede resultar interesante. A lo largo de este último y breve capítulo intentaremos explorar las posibilidades que se abren para defender nuestra privacidad, pues no me resisto a la idea de promover alguna acción que nos encamine si no a una solución directa que defienda nuestros derechos, sí por una senda por la que poco a poco vayamos introduciendo esta preocupación en la agenda pública, en donde ha sido suprimida y silenciada de forma intencionada. Lo hago porque la posibilidad de que no se proponga nada por miedo a que nuestro interlocutor piense erróneamente que le estamos dando órdenes me resulta aún peor que aportar ideas de acción que puedan malinterpretarse.

Toda medida que preserve nuestros derechos y libertades básicas será bienvenida, toda medida que ayude a que la lucha por preservarlas cale en la sociedad será bienvenida: desde la neutralidad de la red hasta la oposición sistemática a la extensión de la restricción de copia y la censura en los controles impuestos en la red para la defensa de la propiedad intelectual; desde la lucha por la

atomización de una Internet que se concentra cada vez más en unos pocos nodos hasta la exigencia a nuestros políticos de que preserven el sistema de voto tradicional y no introduzcan el voto electrónico, fácilmente manipulable.

Porque un poder excesivo en las manos equivocadas puede dar origen a situaciones indeseadas y al abuso de ese poder, porque en tres días de marzo de 2004 utilizamos nuestra libertad de expresión para difundir información y organizar propuestas contra una manipulación informativa manifiesta de nuestros gobernantes y, más importante aún, porque si en algún momento del futuro necesitásemos hacer uso de esa misma libertad de expresión y de movimiento para volver a protestar debemos tener las herramientas necesarias. Y lo único que nos permite mantener estas herramientas es la libertad de expresión y de información: libertad para comunicarnos en una red que no censure nodos, libertad para copiar información en una red que no prohíba la copia.

En la sociedad digital es más que evidente que la defensa de lo que en muchos ámbitos se denominan ciberderechos no es sino la defensa de los derechos civiles más elementales. Puede que hasta 2008 sea posible hacer uso

de las libertades civiles sin recurrir a medios digitales de información, aunque esto no estará exento de dificultades. Lo que podemos asegurar sin miedo a equivocarnos es que esta situación se complicará más cuando todas nuestras comunicaciones (desde la telefonía a la simple conversación por mensajería instantánea) se produzcan en la red. Aún será posible organizar una protesta sin la red, pero ante cualquier abuso partiremos en una posición de desventaja enorme frente a aquellos que llevan a cabo esas acciones que queremos reprobar y que si dispondrán de la red como herramienta para divulgar rápidamente ese mensaje equivocado contra el que queremos luchar.

Cuando digo esto no quiero decir que una nueva revolución dependa de las libertades digitales, más bien es la ausencia de revolución lo que depende de nuestras libertades. No es que pretendamos cambiar el mundo, es que la sociedad digital es radicalmente diferente a la que conocíamos y para aceptar sus bondades no hace falta una revolución, y mucho menos una violenta. En esta situación, el inmovilismo de los viejos poderes, que se ve alentado por las sucesivas reformas legales que acotan la red y levantan vallas de propiedad y restricción donde antes no las había,

es nuestro mayor obstáculo. Podría decirse que en esta ocasión no sería la revolución la que causaría problemas sociales, sino que los conflictos sociales que tenemos actualmente en materia de libertades y privacidad son fruto de la negación y represión silenciosa de los cambios que acontecen en nuestro mundo.

8.1. Valorar y frenar

El punto de partida de todo análisis de este tipo debe ser, sin duda, una necesidad. ¿Qué necesitamos? ¿Qué nos ha traído hasta aquí? Se trata de una pregunta imprescindible sin la que correríamos el riesgo de precipitar nuestras acciones y remitir nuestras quejas al lugar equivocado.

8.1.1. Valorar nuestra privacidad

Necesitamos que nuestras libertades y nuestros derechos estén protegidos. Para lograrlo necesitamos inducir las reformas legales que sean pertinentes. Para que nazca un movimiento social y exija la protección de un derecho debe valorar ese derecho. Si no vemos que lo que estamos perdiendo es algo valioso, ¿saldremos a la calle? No.

Del mismo modo que la gente valora su cultura y se

opone, quizá de forma caótica y mal organizada, a las medidas que desde el poder se toman para favorecer a unos pocos sin tener en cuenta el interés general, antes de intentar ir un paso más allá necesitamos valorar nuestra privacidad. Mientras no entendamos como sociedad todo lo que nuestra privacidad representa, no saldremos a protestar adecuadamente para defenderla.

No será una tarea fácil, ya que desde todas las instancias públicas se nos transmite el mensaje de que nuestra privacidad no es más importante que la seguridad, ignorando la realidad de que en multitud de ocasiones nuestra seguridad va unida precisamente a nuestra privacidad y que en la mayoría de los casos lo que se publicitan como medidas de seguridad ciudadana son en realidad medidas para defender al Estado de sus ciudadanos. La política del miedo y la coerción panóptica están plenamente vigentes y la poderosa maquinaria de la propaganda ayuda a divulgar esos mensajes.

Tampoco será fácil oponerse con un sector privado que, al amparo de la red y de los nuevos servicios publicitarios, ansía conocerlo todo sobre nosotros para segmentar la publicidad que recibimos. Estas empresas nos

envían el mensaje de que nuestra privacidad no vale nada y que podemos cambiarla por cuatro chucherías. La realidad es que estas empresas utilizan nuestros datos para obtener cuantiosos beneficios y bien podría darse el caso de que nuestro empleo dependiera de que nuestro contratante no tenga acceso a nuestro genoma y no pueda saber si tenemos tendencia a padecer una enfermedad. Quizá tampoco queramos que sepan si tenemos o dejamos de tener algún hábito que ellos consideren negativo o punible. Aún tenemos sanidad pública, pero en un contexto de feudalización social y privatización de la sanidad, si intentamos contratar un seguro médico la aseguradora nos cobrará mucho más si tiene un mayor acceso a nuestros datos y conoce nuestros pequeños problemas de salud. Si no impedimos ahora que tengan acceso a toda esa información sobre nosotros, quizá más adelante nos acordemos de todas las ocasiones que tuvimos de defender nuestra privacidad.

Así que, aunque desde las instancias públicas se nos inste a renunciar a nuestra privacidad en nombre de una falsa seguridad y desde las instancias privadas se nos inste a renunciar a la misma porque no es importante, la verdad es la privacidad es la que mantiene al estado policial un poco

más alejado de nosotros y los abusos de compañías sin escrúpulos al otro lado de la valla. Y valorar nuestra privacidad es la piedra angular de la lucha que nos exigen para defenderla.

8.1.2. Es más fácil frenarlo antes

Necesitamos poder permanecer fuera de control, no como declaración de caos, sino como reivindicación de la potestad de decidir cuándo queremos que alguien pueda contactar con nosotros y cuándo queremos permitir que nuestras actividades sean conocidas por otras personas; sobre todo, y como derivado de lo anterior, necesitamos control para decidir cuándo no queremos que esto suceda. Por este motivo es especialmente importante manifestarse contra todas las medidas que conllevan la inclusión de sistemas que hacen posible la recolección continua de información sobre nosotros sin que esté podamos detener y desactivar estos sistemas a voluntad.

Ahora es el momento de frenar estas reformas. Las reformas que se realizan sobre un sistema del tipo que sea siempre son percibidas como tales por quienes han conocido otra forma de funcionamiento de ese sistema determinado.

Una vez entren en funcionamiento, una parte de la población desarrollará tolerancia a estos sistemas, dejará de percibirlos como algo externo y, por tanto no se planteará, resistir. El porcentaje de personas que desarrollan esta tolerancia es mayor en las generaciones que vendrán después y que convivirán con ellas desde su nacimiento.

Por ese motivo es especialmente importante que las reformas encuentren nuestra oposición justo ahora, porque dentro de veinte años toda una generación habrá crecido habituada a no tener privacidad, interiorizará la presencia de videocámaras y la ausencia de intimidad en las comunicaciones. Verán lógico que haya controles biométricos o de RFID delante de cada puerta y que en todo momento un sistema almacene la información relativa a su ubicación actual. En una situación semejante necesitarían una revolución para recuperar los derechos perdidos, pero no habrán conocido otro mundo y les será más difícil imaginarlo; y eso es precisamente lo que a lo largo de la historia ha frenado las revoluciones.

La mejor manera de combatir y defender nuestra privacidad es, por tanto, frenar la introducción de todas las normas que la reducen. Necesitamos luchar para frenar

legalmente estas reformas. Ésa es la idea. No se puede desinventar la rueda y la tecnología está aquí para quedarse. Necesitamos leyes que regulen su uso cuándo éste reduce nuestros derechos.

8.2. Divulgando el mensaje

Una de las situaciones indeseables que se han producido con el advenimiento de la sociedad digital es que los partidarios de continuar con los derechos tal y como los conocíamos y los partidarios de imponer controles han comenzado a actuar cada uno por su lado y han empezado a dirigir sus acciones: unos imponiendo controles, otros averiguando cómo saltarlos; unos usando su influencia política y económica para penalizar toda respuesta no deseada a un control, otros usando los subterfugios que aún permiten los tiempos para seguir saltando controles.

En el camino se quedan cada vez más personas que no poseen la capacidad para saltarse estos controles ni el tiempo necesario para desarrollarla. En el camino se queda, por tanto, parte de nuestra libertad a cada nuevo peldaño que se escala: nuevo control, nuevo salto, nuevo grupo de gente excluida del salto. Esta tendencia no nos beneficia, y el

que piense que no es trascendente es que no ha pensado que quizá sea él quien carezca de la posibilidad de saltar esa nueva barrera. Nuestra libertad no es total si no somos todos libres; el acceso a la cultura no es tal acceso a la cultura si cada vez hay más gente excluida de este acceso; nuestra valoración de la privacidad no es suficiente si no todos la valoran. Para tener opciones de éxito, nuestra visión tiene que ser visible y accesible: hay que divulgar el mensaje.

La manera de conseguir que nuestras libertades sean respetadas no es inventar un nuevo truco para esquivar el último sistema anticopia, aunque eso sea necesario mientras esperamos tiempos mejores en que estas restricciones no estén permitidas. La manera de conseguir que nuestras libertades sean respetadas es entablar un debate entre los partidarios de controlar el sistema y los partidarios de vivir en una sociedad digital basada en protocolos acordados entre todos. Para llegar a esa negociación con posibilidades de éxito necesitamos que nos acompañen muchas voces.

La necesidad de entablar un debate no debe entenderse como la necesidad de reunir en torno a una mesa a representantes de todo el espectro ideológico y

representantes de todos los sectores económicos implicados para alcanzar una solución pragmática y equidistante que no solucionaría nada. El debate que hay que entablar hay que entenderlo como se deben entender las cosas en un entorno digital: comunicándonos de forma activa con nuestro entorno, actuando como nodos de nucleación que den lugar a un debate que vaya creciendo. No están los tiempos para celebrar una reunión bicéfala ni bilateral, sobre todo porque esa mesa estaría llena de gente que probablemente no estaría dispuesta a entender. Si hay algo en lo que podemos ser líderes y sobrepasar ampliamente a los que desde el sistema promueven el control eso es nuestra capacidad de organizarnos, colaborar, participar, ser activos y activistas. Y eso es lo que necesitamos: ser activistas.

8.2.1. Ciberactivismo distribuido: problema y solución

David de Ugarte en su libro *El poder de las redes* afronta esta gran agilidad para el escándalo y el advenimiento de los nuevos sistemas de propagación de la información, así como la *plurarquía* que representan, definida como una suerte de democracia extrema en la que desaparece el derecho a veto y las mayorías no pueden

imponer una postura a las minorías.[168]

Sin embargo, y pese al optimismo con que David nos lo describe, esta plurarquía no parece tampoco la solución definitiva a nuestro problema. Las redes, la distribución de los canales de transmisión y la turba que se genera han demostrado su capacidad para movilizar a la población, pero se han mostrados ineficaces a la hora de prolongar su acción en el tiempo. Los manifestantes de Seattle contra la cumbre de la OMC lograron detener aquella cumbre y trasladar un mensaje, pero no han logrado articular un debate que les permita oponerse adecuadamente a las medidas de liberalización y falsa globalización promovidas por los Estados; han fallado a la hora de entablar las negociaciones necesarias que permitan alcanzar un acuerdo que calme y contente a todos.

Quizá no lo logran porque no lo buscan. Quizá, tal y como exigen los zapatistas de Chiapas, tan sólo quieren *«un mundo en el que quepan muchos mundos»* y eso es irreconciliable con un debate articulado que promueva un único mensaje alternativo, un pensamiento único para el siglo XXI que, por otra parte, no sería deseable, ya que sería como cambiar de collar al perro. Las causas de esta

ineficacia articuladora de nuestro sistema distribuido podrían ser infinitas, pero la consecuencia es sólo una: la humedad de las protestas resbala por el impermeable imperturbable del sistema, aunque éste necesite en ocasiones algo más de tiempo para secarse.

De ello deducimos que no es suficiente con poder gritar una negación, y posiblemente una negación más violenta. Si no va de la mano de una alternativa ejecutable, solamente dará pie a una represión más enérgica por parte de aquellos que pretenden rediseñar el sistema. La negación sin avances sirve para una emergencia, pero no es el camino.

Sin embargo, el ciberactivismo, entendido como la idea de una sociedad abierta y transparente construida de mutuo acuerdo entre todos y a la que todos pueden sumarse, es la base misma de la solución. Porque una sociedad así construida, abierta, libre y participativa, no podría no obedecer a los deseos de aquellos que la están construyendo. Y estos deseos pasarán casi inevitablemente por el respeto de los derechos básicos de todos los implicados en su construcción. Es ahí donde el ciberactivismo adquiere su validez: cuánta más gente esté involucrada en el desarrollo y nuevo cuño de la sociedad digital, más fiable será la misma;

cuánto más claro sea el debate, más justo será. El ciberactivismo pretende, en último término, fomentar que mucha más gente se sume y proponga sus ideas y exprese sus opiniones. Cuanta más gente ponga sus manos en el molde que queremos usar, más gente estará contenta con el resultado obtenido.

8.3. Tecnología contra tecnología

Mientras todo lo anterior da sus frutos, y no será un proceso sencillo, el uso de tecnología para protegernos de la misma será algo absolutamente necesario. Como medida adicional de autoprotección a efectuar mientras se consigue avanzar en la protección de nuestra privacidad tenemos una serie de opciones que nos pueden ayudar a protegernos. Estas opciones rara vez ofrecerán una protección total y podrían estar supeditadas a que la autoridad nos obligue a no utilizarlas. Ya hemos mencionado que cuando hablan de seguridad se refieren sobre todo a la seguridad del Estado, más que a la de las personas. Pese a todo, mientras estén a nuestro alcance las utilizaremos. Mientras llegan las leyes que defiendan nuestros derechos, la tecnología será nuestro único aliado. Tecnología contra tecnología.

8.3.1. Software libre y cifrado

Es posible que en determinados ocasiones estas soluciones les resulten a algunas personas algo muy técnico (aunque esta percepción no sea real): es el caso del cifrado asimétrico de nuestro correo electrónico que impide que sea leído por los robots que revisan la red. Sin embargo, muchas otras soluciones no requieren habilidades ni conocimientos especiales.

Una de las medidas prioritarias consiste en independizarnos completamente cuando usamos nuestras computadoras. Es muy habitual que el software privativo espíe lo que hace el usuario, recogiendo información personal del mismo para enviarla a los servidores del fabricante, que de esta forma verifica que el usuario no está violando en ningún momento la restrictiva licencia de uso que impone previamente al uso del software. En estas circunstancias, nuestras actividades en la red, la información sobre el software que tenemos instalado en nuestro computador y sobre el contenido de nuestro disco duro son enviadas a una empresa privada para que verifique si estamos obedeciendo sus designios.

Se trata de una violación de nuestra privacidad que

no podemos permitir y hasta el momento sólo el uso de software libre cuyo código puede ser auditado nos garantiza que no estamos siendo espiados por la compañía que lo diseña ni por agencias de espionaje gubernamentales.

8.3.2. Resistir cuando esto sea posible

No es suficiente con resistir a la invasión de nuestra intimidad contenida en nuestro ordenador. Con el incremento del número de videocámaras, chips RFID, sistemas de identificación biométrica y el aprovechamiento que se hace de absolutamente todos los espacios de nuestra vida para conocernos mejor e incluir publicidad, la necesidad de crear, mantener y afirmar zonas donde nadie pueda entrar sin nuestro permiso se vuelve acuciante.

Algunos de los documentos que nos identifican (transpondedores para entrar a la oficina, tarjetas de crédito), incluso documentos oficiales como el pasaporte electrónico, incluyen microchips de identificación mediante RFID. Protegerlos de forma que sólo sean leídos cuando sea estrictamente necesario y únicamente por el personal a quien nosotros se lo permitamos es una de las medidas que debemos adoptar.

También hay que rechazar las tarjetas de fidelización que permiten al supermercado reunir una cantidad ingente de información sobre nosotros y mercadear con ella. Las ventajas de estas tarjetas están poco claras y en último término estaríamos vendiendo nuestra información a cambio de una cantidad mínima de dinero ahorrado.[169] A esto se puede responder con una pregunta que nos devuelve al principio de este capítulo: ¿compensa un mínimo ahorro la entrega de toda esa información? ¿Valoramos adecuadamente nuestra privacidad?

8.3.3. Divulgar el mensaje

Realmente las cosas están cambiando, y no es menos real que el estado final en el que nuestra sociedad va a quedar configurada está aún por decidir. Esas dos afirmaciones son algo en lo que podemos estar de acuerdo, pero es importante que todo el mundo sepa que estas cuestiones cruciales se están decidiendo ahí fuera y ahora mismo, y que el perfecto desarrollo de los acontecimientos necesita que todos seamos conscientes de ello y aportemos nuestro pequeño granito de arena.

La tecnología es una herramienta que podemos

utilizar para esta tarea. La misma tecnología que nos obliga a reclamar nuestra privacidad como un derecho moderno es la que nos permite transmitir el mensaje y participar en el diseño de una sociedad digital que se organice de forma más horizontal y limpia, transparente y respetuosa con la voluntad y los intereses de las personas. Por eso abrazamos las tecnologías de la información como la gran arma de que disponemos. Para divulgar el mensaje también sirve la "tecnología contra tecnología". La red todavía permite la libertad de expresión, usémosla. Frente a la amenaza de la sociedad de control, la voz y la acción de todos nosotros cuenta; para subvertir la sociedad de control, toda organización alternativa y distribuida cuenta. Conviértete en un nodo de la red, sé independiente, transmite tu visión de las cosas, resiste al control, activa a tu entorno.

9. Epílogo

Y así hemos llegado hasta aquí. Siempre pensé que con el tiempo escribiría un libro de poesía o una novela, siquiera una breve; sólo ahora que tengo este libro entre las manos me doy cuenta de que la realidad, una vez más, ha demostrado ser esquiva y aquí está mi primer libro cargado de historias que no esperaba tener que contar. Vivimos en una sociedad digital en la que las redes ganan peso paulatinamente en todos los ámbitos. Esto abre nuevas oportunidades para rediseñar el modo en que nuestra sociedad se organiza y ahora son posibles formas de comunicación y gobierno mucho más democráticas. Pero todo esto -la revolución digital, el poder de la red- no es más

que una posibilidad, la de que todo cambio pendiente de realizarse sea a mejor. La realidad es que nadie nos regalará esas mejoras, sino que habrá que luchar para conseguirlas. La buena noticia es que todo eso ya está aquí, y la lucha se centra no tanto en conseguir un derecho del que carecemos como en afianzar aquellos que la tecnología nos ha descubierto. No es fácil, en absoluto, pero hay motivos para no ser pesimista.

No podemos desinventar la rueda, ni la electrónica, ni los *routers*, ni la RFID. Rechazar todas las tecnologías cuyo abuso hace peligrar nuestros derechos y libertades es un error. No hay que rechazar todo lo que tantos años de trabajo nos ofrecen, tan sólo hay que conseguir un uso reglado y responsable de todas esas tecnologías. La sociedad digital está aquí para quedarse y carece de sentido intentar mantener los viejos sistemas que han servido hasta ahora para gestionar la sociedad en épocas pasadas. Más aún, no es que carezca de sentido, es que supone una acción peligrosa y arriesgada con la que tenemos muy poco que ganar y mucho que perder.

Esta certeza de que no podemos eliminar todo aquello que nos rodea es la que nos obliga a blindar

adecuadamente nuestras libertades frente al imparable avance de la tecnología y el abaratamiento de sistemas de control más potentes, que hace que sean más accesibles. En un mundo donde todo queda registrado en múltiples sitios es muy importante tener un control de quién tiene acceso a toda nuestra información personal, así como las condiciones de acceso. También será necesario definir las responsabilidades legales, civiles y penales de todo el que haga un mal uso de nuestra información privada.

No es que el ciberespacio no nos ofrezca libertad, no es como si nunca hubiese sido declarado libre por Barlow en un manifiesto que muchos hicimos nuestro y que aún nos emociona leer tantos años después,[170] es que quizá no está resultando tan sencillo mantener a los Estados lejos del ciberespacio y del entorno de libertad que ha generado para el desarrollo de nuestras vidas.

El blindaje de nuestras libertades no vendrá de la mano de nuevas medidas de contratecnología. La contratecnología es un mal necesario, una suerte de desobediencia civil ante lo obsceno del estado actual de la privacidad, una autodefensa inevitable en tanto las leyes no nos defiendan adecuadamente. El blindaje de nuestras

libertades no puede venir por otra vía que no sea la de la redacción de leyes justas que fijen los principios que habrán de respetar la libertad en la sociedad digital. Mientras esto llega, la tecnología nos ofrece una protección, débil pero existente después de todo.

El desarrollo de estas leyes conllevará -no hay otra alternativa- el desarrollo e inclusión de toda una batería de protocolos que regirán las actividades de todos y cada uno de nosotros, que servirá de garante de la democracia al perseguir adecuadamente a todos los delincuentes que cometan abusos contra el resto de ciudadanos, sin perder de vista que estos delincuentes que cometan abusos bien podrían ser las fuerza del orden del Estado en el caso de que se excedan en el ejercicio de sus funciones o abusen de su posición. No deben existir excepciones.

Para conseguir que esto tenga efectos prácticos hay que luchar por la armonización en esta materia. Del mismo modo que quienes pretenden imponer la sociedad bajo vigilancia utilizan la *armonización interestatal* como herramienta para empeorar nuestra situación civil o económica, nosotros debemos organizar una protesta que garantice que los mismos derechos digitales que nosotros

tengamos reconocidos y respetados sean también reconocidos y respetados en todas las zonas del mundo; como reza el viejo proverbio: «Cuando un hombre está preso injustamente, ningún hombre está libre del todo». La manera de lograrlo es conseguir que se incluyan referencias claras a la defensa de nuestros derechos en los textos legales que habrán de escribirse en los días por venir y que darán forma a nuestro mundo cuando éste se adapte a los cambios que ya ha sufrido.

Sin embargo, y pese a lo que hemos ido viendo a lo largo de este texto, hay motivos para mantener la cabeza alta y ser optimista: la lucha por las libertades es una lucha perpetua y, en el peor de los casos, nunca se pierde del todo. Diríase que a nosotros nos parece que el mundo va a peor, pero a una persona mayor podría parecerle que el mundo siempre ha caminado sobre el filo de la navaja. Si atendemos a esta segunda visión, una derrota en un momento determinado puede ser siempre remontada si colaboramos entre todos para superar los problemas que de ella se puedan derivar, aunque esto no justifica en modo alguno la desidia que pueda encaminar a una derrota. Que a las generaciones por venir les pueda ir mejor no significa que

no podamos conseguir una victoria que nos ayude a ver satisfechas algunas de nuestras aspiraciones. Ellos tienen todos los controles y nosotros tenemos todas las propuestas. Ahora sólo hay que hacer todo lo posible, empezando por las pequeñas cosas que en nuestra vida cotidiana nos ayudarán a nosotros mismos, para que las cosas salgan bien. Esta vez ganaremos. ¡Salud!

Referencias

1 Siva Vaidhyanathan, *The anarchist in the library*, Ed. Basic Books, 2004.

2 George Akerlof, “The Market for 'Lemons': Quality Uncertainty and the Market Mechanism”, *Quarterly Journal of Economics* 84 1970, pág.488–500.

3 Diccionario de la Real Academia Española de la Lengua, DRAE, 22ª edición.

4 Diccionario de la Real Academia Española de la Lengua, DRAE, 22ª edición.

5 Glee Harrah Cady y Pat McGregor, *Protect your digital privacy*, Ed. Que, 2002, pág. 39. (ISBN: 0-7897-2604-1)

6 Scott McNealy es director ejecutivo (CEO) de *Sun Microsystems*; más información disponible online en http://www.sun.com/aboutsun/executives/mcnealy/bio.jsp, accedido el 19 de enero de 2008.

7 Scott McNealy, *McNealy calls for smart cards to help security*, *ComputerWorld*, 12 de octubre de 2001, disponible online en http://www.computerworld.com/securitytopics/security/story/0,10801,64729,00.html, accedido el 25 de diciembre de 2007.

8 Sara Kehaulani Goo, *Washington Post*, 2004, disponible online en http://www.washingtonpost.com/wp-dyn/articles/A17073-2004Aug19.html, accedido el 19 de agosto de 2007.

9 David de Ugarte, *El poder de las redes*, El Cobre, 2007, ISBN: 978-84-611-8873-4

10 David de Ugarte, *El poder de las redes*, El Cobre, 2007, ISBN: 978-84-611-8873-4

11 Siva Vaidhyanathan, *The anarchist in the library*, Ed Basic

Books 2004.

12 Tim Berners-Lee, *Weaving the web*, Ed. Harper, San Francisco 1999.

13 José María Rodríguez Paniagua, *La democracia moderna y la distinción de moral y Derecho*, *Doxa: Cuadernos de filosofía del derecho* 1, 1994, págs. 307-320.

14 Robert Darnton, "Paris: the early Internet", *New York Review of Books*, vol. 47, nº. 11, 29 de junio de 2000, disponible online en http://www.nybooks.com/articles/27/, accedido el 10 de enero de 2008.

15 Robert Darnton, *The forbidden best-sellers of pre-revolutionary France*, Ed. Norton, 1995, ISBN: 0-393-31442-1

16 R. J. Rummel, *Death by government*, Transaction Publishers, 1994.

17 *El Mundo*, "Diversas ONG critican a Yahoo! por desvelar datos de disidentes chinos", 28 de agosto de 2007, disponible online en http://www.elmundo.es/navegante/2007/08/28/tecnologia/1188293654.html, accedido el 7 de diciembre de 2007.

18 Naomi Klein, *La doctrina del shock*, Paidós, 2007.

19 Naomi Klein, *La doctrina del shock*, Paidós, 2007.

20 Bruce Schneier, *Beyond fear: Thinking sensibly about security in an uncertain world*, Copernicus Books, 2003, ISBN 0-387-02620-7

21 *BBC News*, "Scandal-hit US lawmaker in rehab", 2 de octubre de 2006, disponible online en http://news.bbc.co.uk/2/hi/americas/5399724.stm, accedido el 8 de diciembre de 2007.

22 Jeremy Bentham, *The panopticon writings*, Ed. Miran Bozovic, 1995.

23 Ver apartado dedicado al «cercamiento digital» en este

libro, para más información.

24 Jesús Requena Hidalgo, “De la «sociedad disciplinaria» a la «sociedad de control»: la incorporación de nuevas tecnologías a la policía”, *Scripta Nova*, vol. VIII, nº. 170 (43), 1 de agosto de 2004, ISSN: 1138-9788

25 *Público*, “Bush justifica los interrogatorios de presuntos terroristas con la técnica de la ‘asfixia simulada’”, 15 de febrero de 2008, disponible online en http://www.publico.es/049003/bush/justifica/interrogatorios/presuntos/terroristas/tecnica/asfixia/simulada, accedido el 16 de febrero de 2008.

26 *El Universal*, “Estados Unidos endurece medidas de control antiterrorista”, 4 de agosto de 2007, disponible online en http://www.eluniversal.com/2007/08/04/int_art_estados-unidos-endur_391198.shtml, accedido el 14 de abril de 2008.

27 Jorge Casanova, “Sanidad de pago para obesos y fumadores”, *La voz de Galicia*, 3 de junio de 2003, disponible online en http://www.lavozdegalicia.es/hemeroteca/2003/06/03/172482 4.shtml, accedido el 7 de diciembre de 2007.

28 *ABC*, “Los obesos tendrán que pagar más impuestos en Finlandia”, 10 de febrero de 2007, disponible online en http://www.abc.es/hemeroteca/historico-10-02-2007/abc/Internacional/los-obesos-tendran-que-pagar-mas-impuestos-en-finlandia_1631391828618.html, accedido el 7 de diciembre de 2007.

29 *Privacy International*, “Leading surveillance societies in the EU and the World 2007. The 2007 International Privacy Ranking”, 28 de diciembre de 2007, disponible online en http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597, accedido el 16 de febrero de

2008.

30 J. M. Martí Font, “Sarkozy propone un «nuevo contrato social»”, *El País*, 19 de septiembre de 2007, disponible online en http://www.elpais.com/articulo/internacional/Sarkozy/propone/nuevo/contrato/social/elpepuint/20070919elpepiint_1/Tes , accedido el 7 de diciembre de 2007.

31 Recibió su nombre del eurodiputado que la impulsó, puede consultarse online en http://eur-lex.europa.eu/LexUriServ/site/es/com/2004/com2004_0002es01.pdf, accedido el 7 de diciembre de 2007.

32 Campaña *Stop Bolkestein!*, se puede consultar un seguimiento de la misma en *Attac Madrid*, disponible online en http://www.attacmadrid.org/indicedin/indicedin.php?p=62, accedido el día 16 de febrero de 2008.

33 “Violencia simbólica” es el concepto con que Pierre Bourdieu define este tipo de adoctrinamiento educativo.

34 Bill Carter, “Pentagon on pictures of dead troops is broken”, *The New York Times*, 23 de abril de 2004, disponible online en http://query.nytimes.com/gst/fullpage.html?res=980CE6DD153AF930A15757C0A9629C8B63, accedido el 6 de marzo de 2008.

35 Naomi Klein, *Vallas y ventanas*, pág. 143, Editorial Paidós, 2002.

36 *Jukebox*, clásica máquina de música en la introduces una moneda y reproduce una única canción previamente escogida.

37 Hitachi µ-chip, el microchip RFID más pequeño del mundo (en el momento de ser escrito este texto) fue presentado el 6 de febrero de 2006. Información online disponible en

http://www.hitachi.co.jp/Prod/mu-chip/, accedido el 8 de diciembre de 2007.

38 Charles Walton, “Electronic Identification & Recognition System”, Patente número 3752960, agosto de 1973.

39 En Málaga, Madrid y Barcelona no tienen nombre especial, en Londres la Oyster Card incluye RFID, al igual que Navigo en París.

40 Ministerio del Interior, http://www.mir.es/SGACAVT/pasaport/Pasaporte_electronico.html accedido el 24 de agosto de 2007.

41 Mark Roberti, “RFID reaches the legal limit”, *RFID Journal*, 2 de octubre de 2006, disponible online en http://www.rfidjournal.com/article/articleview/2692/1/128/, accedido el 9 de marzo de 2008.

42 Información electrónica ampliada sobre Oyster Card, https://www.oystercard.com; Tarjeta 7 Colinas, http://www.carris.pt/index.php?area=balcao&subarea=passes_e_bilhetes_7colinas; y Navigo, https://www.navigo.fr.

43 Patente concedida a International Business Machines Corporation. Nombre: “Identification and tracking of persons using RFID-tagged items”. Patente número: US20020165758 concedida el 7 de noviembre de 2002 en Estados Unidos.

44 Solicitud de patente por Apple Computers Inc. con nombre RFID Network Arrangement, disponible online en http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1="20070054616".PGNR.&OS=DN/20070054616&RS=DN/20070054616, accedido el 7 de diciembre de 2007.

45 Reporteros sin Fronteras, “Handbook for bloggers and cyber-dissidents”, disponible online en http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf, accedido el 6 de marzo de 2008.

46 http://www.verichipcorp.com/

47 *Wired*, “Cyborg 1.0”, febrero de 2000, disponible online en http://www.wired.com/wired/archive/8.02/warwick.html, accedido el 8 de diciembre de 2007.

48 Amal Graafstra, “Hands on”, *IEEE Spectrum*, marzo 2007, disponible online en http://www.spectrum.ieee.org/print/4940, accedido el 8 de diciembre de 2007.

49 Paul Miller, “VeriChip chipping 200 Alzheimer's patients for RFID VeriMed trials”, *Engadget*, 4 de septiembre de 2007, disponible online en http://www.engadget.com/2007/09/04/verichip-chipping-200-alzheimers-patients-for-rfid-verimed-tria/, accedido el 8 de diciembre de 2007.

50 Steven Deare, “RFID to track ACT prisoners”, *Indimedia UK*, 9 de junio de 2006, disponible online en http://www.indymedia.org.uk/en/2006/06/342359.html, accedido el 8 de diciembre de 2007.

51 *BBC News*, “Barcelona clubbers get chipped”, 29 de septiembre de 2004, disponible online en http://news.bbc.co.uk/2/hi/technology/3697940.stm, accedido el 8 de diciembre de 2007.

52 K.C. Jones, “California bans forced RFID implants for humans”, 15 de octubre de 2007, *Information Week*, disponible online en http://www.informationweek.com/story/showArticle.jhtml?articleID=202402856&cid=RSSfeed_IWK_News, accedido el 8 de diciembre de 2007.

53 George Ou, “Why the ban on mandatory RFID implants should be federal?”, *ZDNet*, 13 de septiembre de 2007, disponible online en http://blogs.zdnet.com/Ou/?p=750, accedido el 8 de diciembre de 2007.

54 *ZDNet*, 15 de septiembre de 2007, disponible online en http://talkback.zdnet.com/5208-10533-0.html;jsessionid=_OqVjg029ig3iNZWAr?forumID=1&threadID=38731&messageID=711012&start=-9856, accedido el 8 de diciembre de 2007.

55 *Washington Post*, “Chip implants linked to animal tumors”, 8 de septiembre de 2007, disponible online en http://www.washingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html , accedido el 8 de diciembre de 2007.

56 “Cómo clonar un VeriChip”, disponible online en http://cq.cx/verichip.pl, accedido el 17 de febrero de 2008.

57 Ben Charmy, “RFID cell phone takes shape on Nokia”, *ZDNet News*, 25 de octubre de 2004, disponible online en http://news.zdnet.com/2100-1035_22-5424528.html, accedido el 8 de diciembre de 2007.

58 Sue Reid, “'Safest ever' passport is not fir for porpose”, *The Daily Mail*, 5 de marzo de 2007, disponible online en http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=440069&in_page_id=1770, accedido el 17 de febrero de 2008.

59 Brian Brady, “Prisoners to be chipped like dogs”, *The Independent*, 13 de enero de 2008, disponible online en http://www.independent.co.uk/news/uk/politics/prisoners-to-be-chipped-like-dogs-769977.html, accedido el 3 de febrero de 2008.

60 New Scientist Tech, “Big Brother is Listening to you”, 21 de noviembre de 2006, disponible online en

http://technology.newscientist.com/article/mg19225780.159, accedido el 3 de febrero de 2008.

61 *Times Online*, *Military junta threatens monks in Burma*, 24 de septiembre de 2007, disponible online en http://www.timesonline.co.uk/tol/news/world/asia/article2521951.ece, accedido el 3 de febrero de 2008.

62 15 de febrero de 2003, manifestación global contra la invasión de Irak con más de diez millones de manifestantes en todo el mundo.

63 Mark Ballard, "Beer fingerprints to go UK-wide", *The Register*, 20 de octubre de 2006, disponible online en http://www.theregister.co.uk/2006/10/20/pub_fingerprints/, y accedido el 12 de enero de 2008.

64 Pepe Cervera, "NSA y la falacia del político", *20 Minutos*, 12 de mayo de 2006, disponible online en http://blogs.20minutos.es/retiario/post/2006/05/12/nsa-y-falacia-del-politico, accedido el 9 de marzo de 2008.

65 Marc van Gurp, http://blogger.xs4all.nl/marcg/archive/2007/01/21/175733.aspx, accedido el 9 de marzo de 2008.

66 Rosie Cowan, Duncan Campbell y Vikram Dodd, "New claims emerge over Menezes death", *The Guardian*, 17 de agosto de 2005, disponible online en http://www.guardian.co.uk/attackonlondon/story/0,16132,1550565,00.html, accedido el 12 de enero de 2008.

67 *Madri+d*, "Control de acceso mediante reconocimiento facial", 26 de marzo de 2007, disponible online en http://www.madrimasd.org/informacionidi/noticias/noticia.asp?id=29700, accedido el 14 de enero de 2008.

68 Proyecto: El empleo de sistemas biométricos para el reconocimiento de personas en los aeropuertos; llevado a cabo entre el 1 de febrero de 2005 y el 1 de febrero de 2006.

Investigador principal: Doctor D. Enrique Cabello Pardos (URJC).

69 *BBC News*, "All UK 'must be on DNA base'", 5 de septiembre de 2007, disponible online en http://news.bbc.co.uk/2/hi/uk_news/6979138.stm, accedido el 8 de diciembre de 2007.

70 *Público*, "La lista única de ADN reabrirá 2.000 violaciones sin esclarecer", 22 de octubre de 2007, disponible online en http://www.publico.es/espana/009082/lista/unica/adn/reabrira/2000/violaciones/esclarecer, accedido el 8 de diciembre de 2007.

71 *Le Monde*, "La tentation du fichage génétique de masse", 25 de septiembre de 2006, disponible en http://www.lemonde.fr/web/article/0,1-0@2-3208,36-816576,0.html, accedido el 8 de diciembre de 2007.

72 Touche pas à mon ADN. http://www.touchepasamonadn.com/

73 Adam Thierer y Clyde Wayne Crews Jr., "Who rules the net? Internet governance and jurisdiction", 2003.

74 Starbug, "How to fake fingerprints?", *Chaos Computer Club*, 25 de octubre de 2004, disponible online en http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en, accedido el 12 de enero de 2008.

75 Jonathan Kent, "Malaysia car thieves steal finger", *BBC News*, 31 de marzo de 2005, disponible online en http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm, accedido el 12 de enero de 2008.

76 Marie Woolf, "DNA database chaos with 500,000 false or misspelt entries", *The independent*, 26 de agosto de 2007, disponible online en http://news.independent.co.uk/uk/politics/article2896193.ece, accedido el 14 de enero de 2008.

77 Nate Anderson, “Nielsen dives into online watermarking, content filtering”, *Ars Technica*, 5 de diciembre de 2007, disponible online en http://arstechnica.com/news.ars/post/20071205-nielsen-dives-into-watermarking-content-filtering.html, accedido el 4 de febrero de 2008.

78 *BBC News*, “'Personal data' on iTunes tracks”, 1 de junio de 2007, disponible online en http://news.bbc.co.uk/2/hi/technology/6711215.stm, accedido el 12 de enero de 2008.

79 Especificaciones de AACS, http://www.aacsla.com/specifications/specs091/AACS_Spec_Prerecorded_0.91.pdf, accedido el 11 de septiembre de 2007.

80 Pepe Cervera, “Las llaves del pc”, *20 minutos*, http://blogs.20minutos.es/retiario/post/2005/11/24/las-llaves-del-pc, accedido el 8 de diciembre de 2007.

81 Eben Moglen, "'Die Gedanken Sind Frei': Free Software and the Struggle for Free Thought Wizards of OS 3 Opening Keynote", Berlín, 10 de junio de 2004, disponible online en http://emoglen.law.columbia.edu/publications/berlin-keynote.html, accedido el 4 de febrero de 2008.

82 Más información en http://fabathome.org/

83 *Indymedia*, “¿Qué pasa con las webs de Batasuna?”, 21 de septiembre de 2002, disponible online en http://euskalherria.indymedia.org/eu/2002/09/1572.shtml, accedido el 12 de enero de 2008.

84 Jorge Cortell, “Los peligros ocultos de la red: La censura III”, *Personal Computer & Internet* nº. 30, junio de 2005, disponible online en http://www.cortell.net/2005/07/04/los-peligros-ocultos-de-la-red-iii-la-censura-pci-30/, accedido

el 12 de enero de 2008.

85 Quinn Norton, “Hackers Con Submits to Spychips”, *Wired*, 28 de diciembre de 2006, disponible online en http://www.wired.com/science/discoveries/news/2006/12/72364, accedido el 8 de diciembre de 2007.

86 http://www.congreso.es/public_oficiales/L8/CONG/BOCG/A/A_128-09.PDF, accedido el 7 de octubre de 2007.

87 Caso Mark Foley, senador republicano acusado de pederastia gracias a unos *logs* de mensajería instantánea que fueron mostrados en público sólo varias semanas antes de las elecciones legislativas de 2006.

88 Steven M. Bellovin, Matt Blaze, Whitfield Diffie, Susan Landau, Peter G. Neumann y Jennifer Rexford, “Risking communications security: potential hazards of the Protect America Act”, *IEEE Security & Privacy*, vol. 6, nº. 1, enero/febrero de 2008, págs. 24-33.

89 *Principio de generación de escasez*. Información electrónica ampliada disponible en http://www.deugarte.com/wiki/contextos/Principio_de_generación_de_escasez, accedido el 6 de marzo de 2008.

90 David Bravo, *Copia este libro*, Dmem S. L., 2005, pág 10.

91 Javier Díaz Noci, “Periodismo y derechos de autor: evolución histórica de la protección jurídica sobre la obra informativa”, *ZER Revista de Estudios de Comunicación* (Universidad del País Vasco), diciembre de 1999, disponible online en http://www.ehu.es/zer/zer7/noci74.html, accedido el 9 de diciembre de 2007.

92 *Statute of Anne* o *An Act for the Encouragement of Learning, by vesting the Copies of Printed Books in the Authors or purchasers of such Copies, during the Times therein mentioned*. Entró en vigor en el Reino Unido el 10 de octubre de 1710.

93 Oscar René Vargas, "¿Qué es el Consenso de Washington?", *El Nuevo Diario*, 13 de noviembre de 2002, disponible online en http://www.lainsignia.org/2002/noviembre/econ_033.htm, accedido el 12 de enero de 2008.

94 Pedro J. Canut, "La cultura libre en el derecho continental (versión 1.1)", *Blogespierre*, 27 de julio de 2005, disponible online en http://www.blogespierre.com/2005/07/27/la-cultura-libre-en-el-derecho-continental-version-11/, accedido el 12 de enero de 2008.

95 Lawrence Lessig, *Por una cultura libre*, Traficantes de sueños (2005).

96 Mike H. Goldhaber, "The attention economy: the natural economy of the net", *First Monday* 2, nº. 4, 1997, disponible online en http://www.firstmonday.org/issues/issue2_4/goldhaber/, accedido el 9 de diciembre de 2007.

97 Marga Zambrana, "Fuertes críticas contra Google por colaborar con la censura en China", *El Mundo*, 25 de enero de 2006, disponible online en http://www.elmundo.es/navegante/2006/01/25/empresas/1138183868.html, accedido el 12 de marzo de 2008.

98 Sylvie Barak, "Google buckles under power of the DMCA", *The Inquirer*, 12 de marzo de 2008, disponible online en http://www.theinquirer.net/gb/inquirer/news/2008/03/12/cowardly-google-should-search, accedido el 12 de marzo de 2008.

99 INE, *Informe sobre uso de bibliotecas*, Instituto Nacional de Estadística, 13 de febrero de 2008, disponible online en http://www.ine.es/prensa/np492.pdf, accedido el 17 de febrero de 2008.

100 Información electrónica ampliada en

http://es.wikipedia.org/wiki/Seguridad_por_oscuridad, accedido el 10 de octubre de 2007.

101 Saul Hansell, "A sigh of relief for blockbuster: Few people copy DVDs", *The New York Times* online, disponible online en http://bits.blogs.nytimes.com/2007/07/12/a-sigh-of-relief-for-blockbuster-few-people-copy-dvds/, accedido el 6 de febrero de 2008.

102 Artículo 25.2, Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril.

103 Felix Oberholzer-Gee y Koleman Strumpf, "The Effect of File Sharing on Record Sales: An Empirical Analysis", *Journal of Political Economy* 115, 2007, págs. 1-42

104 David Blackburn, "Online piracy and recorded music sales", disponible online en http://web.archive.org/web/20051212053259/http://www.economics.harvard.edu/~dblackbu/papers/blackburn_fs.pdf, accedido el 12 de enero de 2008.

105 *Baquia*, "La última fábrica española de CD vírgenes echa el cierre", 30 de diciembre de 2005, disponible online en http://www.baquia.com/noticias.php?id=10426, accedido el 7 de febrero de 2008.

106 David Bravo, http://www.filmica.com/david_bravo, accedido el 7 de febrero de 2008.

107 Pedro J. Canut, http://www.bloguespierre.com, accedido el 7 de febrero de 2008.

108 Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril.

109 *20 minutos*, "Europa impone a España un canon por el préstamo de libros en bibliotecas", 22 de marzo de 2007,

disponible online en http://www.20minutos.es/noticia/214764/, accedido el 12 de enero de 2008.

110 Campaña «No al préstamo de pago», http://exlibris.usal.es/bibesp/nopago/

111 Richard Jones, “Free the Music”, *Last.FM - the blog*, 23 de enero de 2008, disponible online en http://blog.last.fm/2008/01/23/free-the-music, accedido el 7 de febrero de 2008.

112 *20 minutos*, “Europa impone a España un canon por el préstamo de libros en bibliotecas”, 22 de marzo de 2007, disponible online en http://www.20minutos.es/noticia/214764/, accedido el 12 de enero de 2008.

113 Nate Anderson, “DMCA-style laws come to Canada, Switzerland”, *Ars Technica*, 29 de noviembre de 2007, disponible online en http://arstechnica.com/news.ars/post/20071129-dmca-style-laws-come-to-canada-switzerland.html, accedido el 23 de enero de 2008.

114 *Slashdot*, “U.S. Senators Pressure Canada on Canadian DMCA”, 6 de marzo de 2007, disponible online en http://politics.slashdot.org/article.pl?sid=07/03/06/1436223, accedido el 23 de enero de 2008.

115 Richard Stallman, *Software libre para una sociedad libre*, , Traficantes de sueños, 2004, pág. 23.

116 Página web del MIT: http://www.mit.edu/.

117 “Software privativo”, expresión más utilizada por el movimiento de software libre para referirse a todo software no libre.

118 Andres Lomeña, “Entrevista con Richard Stallman”, *Versvs' Blog*, 21 de noviembre de 2007, disponible online en

http://www.versvs.net/anotacion/entrevista-con-richard-stallman, accedido el 17 de febrero de 2008.

119 Richard Stallman, *Software libre para una sociedad libre*, Traficantes de sueños, 2004, pág. 45.

120 http://www.creativecommons.org, accedido a 24 de octubre de 2007.

121 Movimiento por la Devolución, *¿Qué es la devolución?*, Web del Movimiento por la Devolución, disponible online en http://www.devolucion.info/que-es-la-devolucion/, accedido el 7 de febrero de 2008.

122 Lluís Pérez, "Domini Públic, per què? I Creative Commons, per què no?, http://perezlozano.blogspot.com/2006/08/domini-pblic-per-qu-i-creative-commons.html, accedido a 24 de octubre de 2007.

123 El 1 de abril o April's Fools Day es el equivalente al día de los Inocentes en numerosas partes del mundo, principalmente en el mundo anglosajón.

124 "Google bate su record en Bolsa con una ofensiva en la web 2.0", 1 de noviembre de 2007, http://www.cincodias.com/articulo/empresas/Google/bate/record/Bolsa/ofensiva/web/cdssec/20071101cdscdiemp_4/Tes/ , accedido el 6 de noviembre de 2007.

1 [25] *20 minutos*, "Los jóvenes pagarán menos por el seguro del coche si se dejan espiar por satélite", 14 de abril de 2008, disponible online en http://www.20minutos.es/noticia/369042/0/mapfre/gps/espia/, accedido el 9 de julio de 2008.

125 Alrededor de 160.000 euros.

126 *El Mundo*, "Las discográficas ganan una demanda contra una mujer por compartir música en EE.UU.", 5 de octubre de 2007, disponible online en

http://www.elmundo.es/navegante/2007/10/05/tecnologia/1191569327.html, accedido a 26 de octubre de 2007.

127 Naomi Klein, *No Logo*, Ed. Paidós, 2001, pág 39.

128 Katherine Albrecht, *Chips espías*, Grupo Nelson, 2006.

129 Katherine Albrecht, *Chips espías*, Grupo Nelson, 2006.

130 Constance Hays, "What they know about you", *The New York Times*, 14 de noviembre de 2004, disponible online en http://query.nytimes.com/gst/fullpage.html?res=9406E5D7163FF937A25752C1A9629C8B63, accedido el 9 de marzo de 2008.

131 *MSNBC*, "Mini says a 'high-tech hello!' to its drivers", 21 de febrero de 2007, http://www.msnbc.msn.com/id/17009358/ accedido el 11 de noviembre de 2007.

132 Saul J. Berman, Bill Battino, Louisa Shipnuck y Andreas Neus, «The end of advertising as we know it», disponible online en http://t1d.www-03.cacheibm.com/industries/media/doc/content/bin/media_ibv_advertisingv2.pdf, accedido el 11 de noviembre de 2007.

133 Jaikumar Vijayan, "Most consumers clueless about online tracking", *ComputerWorld*, 5 de noviembre de 2007, disponible online en http://www.computerworld.com.au/index.php/id;1726527222;fp;16;fpid;1, accedido el 12 de noviembre de 2007.

134 *Cinco días*, "Google bate su récord en Bolsa con una ofensiva en la web 2.0", 1 de noviembre de 2007, http://www.cincodias.com/articulo/empresas/Google/bate/record/Bolsa/ofensiva/web/cdscdi/20071101cdscdiemp_4/Tes/ accedido el 12 de noviembre de 2007.

135 *Facebook Beacon*, 6 de noviembre de 2007, http://www.facebook.com/press/releases.php?p=9166,

accedido el 13 de noviembre de 2007.

136 Bradley L. Carpenter, Garrett R. Vargas, Krista L. Johnson, Scott Searle, “Advertising Services Architecture”. Solicitud de patente número 20070157227, julio de 2007.

137 Reinón Muñoz, “Francia: Lille 3000, el futuro ya está aquí” *Kaos en la red*, 14 de julio de 2006, disponible online en http://www.kaosenlared.net/noticia.php?id_noticia=20992, accedido el 16 de noviembre de 2007.

138 *El País*, “Una ciudad sin publicidad”, 20 de junio de 2007, disponible online en http://www.elpais.com/articulo/economia/ciudad/publicidad/elpepueco/20070620elpepueco_3/Tes, accedido el 16 de noviembre de 2007.

139 Rick Duris, “Just how big is RFID?”, *Frontline Solutions*, 1 de diciembre de 2003, disponible online en http://findarticles.com/p/articles/mi_m0DIS/is_12_4/ai_112366620 accedido el 18 de noviembre de 2007.

140 *RFID-Spain*, “Las tiendas de Tokio hacen publicidad a través de RFID”, 28 de diciembre de 2006, disponible en http://www.rfid-spain.com/portal/rfid-spain/business_intelligence/Controller?mvchandler=portals&action=dispatch&idInstance=34690&pAction=preview&idPortlet=3144&idPortal=portal2&idSection=1017&jsfInit=null accedido el 18 de noviembre de 2007.

141 *Cinco Días*, «¿Virus en la estantería del supermercado?», 16 de marzo de 2006, disponible en http://www.cincodias.com/articulo/economia/Virus/estanteria/supermercado/cdseco/20060316cdscdseco_4/Tes/ accedido el 22 de noviembre de 2007.

142 *¿Quién vigila al vigilante?*, “Primer contacto físico y fotos de la nevera RFID”, 31 de enero de 2007, disponible online

en http://www.lavigilanta.info/2007/01/primicia-primer-contacto-fsico-y-fotos.html accedido el 12 de febrero de 2008

143 John Williamson, “A short history of the Washington Consensus”, artículo encargado por la Fundación CIDOB para la conferencia "From the Washington Consensus towards a new global governance", Barcelona, 24-25 de septiembre de 2004, disponible online en www.ild.org.pe/files/williamson0904-21.pdf, accedido el 9 de julio de 2008

144 Naomi Klein, *Vallas y ventanas*, Paidós, 2002.

145 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

146 Artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

147 Ana Tudela, “Los datos personales de los españoles hacen las Américas”, *Público*, 1 de noviembre de 2007, disponible online en http://publico.es/dinero/012669/datos/personales/espanoles/americas, accedido el 1 de diciembre de 2007.

148 “QUIS CUSTODIET IPSOS CUSTODES? (¿Quién guarda a los guardias?)”, 15 de julio de 2007, disponible online en http://www.internautas.org/html/4372.html accedido el 29 de noviembre de 2007.

149 José Antonio Hernández, “Sólo el CNI y la policía podrán pedir los datos de las comunicaciones telefónicas”, *El País*, 12 de octubre de 2006, disponible online en http://www.elpais.com/articulo/espana/Solo/CNI/policia/judicial/podran/pedir/datos/comunicaciones/telefonicas/elpporesp/20061012elpepinac_13/Tes/, accedido el 29 de noviembre de 2007.

150 Artículo 14, Constitución Española de 1978.

151 Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

152 Artículo 18, Constitución Española de 1978.

153 Christophe Beaudouin, “Bruxelles veut imposer les statistiques ethniques et s'intéresse à notre vie intime”, *AgoraVox*, 27 de noviembre de 2007, disponible online en http://fr.news.yahoo.com/agoravox/20071127/tot-bruxelles-veut-imposer-les-statistiq-89f340e_1.html accedido el 1 de diciembre de 2007.

154 Bean Leapman, “Three in four young black men on the DNA database”, *Telegraph*, 11 de mayo de 2006, disponible online en http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/11/05/nrace05.xml, accedido el 17 de febrero de 2008.

155 *BBC*, “All UK 'must be an DNA database'”, 5 de septiembre de 2007, disponible online en http://news.bbc.co.uk/1/hi/uk/6979138.stm, accedido el 17 de febrero de 2008.

156 *Público*, “La lista única de ADN reabrirá 2.000 violaciones sin esclarecer”, 22 de octubre de 2007, disponible online en http://www.publico.es/espana/009082/lista/unica/adn/reabrira/2000/violaciones/esclarecer, accedido el 1 de diciembre de 2007.

157 Naomi Klein, *Vallas y ventanas*, Editorial Paidós, pág. 143.

158 *El País*, “Google desvela la identidad de un 'blogger' israelí sin orden judicial”, 28 de noviembre de 2007, disponible online en http://www.elpais.com/articulo/Internet/Google/desvela/identidad/blogger/israeli/orden/judicial/elpeputec/20071128elpepunet_8/Tes, accedido el 1 de diciembre de 2007.

159 Principalmente, la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos

160 Artículo 6 de la Ley Orgánica 4/1997, de 4 de agosto.

161 Instrucción 1/2006 de 8 de noviembre, disponible online en http://www.boe.es/boe/dias/2006/12/12/pdfs/A43458-43460.pdf, accedido el 6 de diciembre de 2006.

162 Nota de prensa de la AEPD, disponible online en https://www.agpd.es/upload/Prensa/nota%20informativa%20Videovigilancia.pdf, accedido el 6 de diciembre de 2007.

163 *La Insignia*, "Informe de OXFAM: Propiedad intelectual y disparidad de conocimientos", 7 de noviembre de 2002, disponible online en http://www.lainsignia.org/2002/noviembre/cyt_001.htm, accedido el 6 de diciembre de 2007.

164 European Commission – External Trade – Trade Issues, *Intellectual Property: EU/US review progress in joint anti-counterfeiting drive; plan to expand work in 2007*, 1 de febrero de 2007, disponible online en http://ec.europa.eu/trade/issues/sectoral/intell_property/pr010207_en.htm, accedido el 6 de diciembre de 2007.

165 Todos contra el canon, http://www.todoscontraelcanon.es

166 Artículo 21 de la Declaración Universal de los Derechos Humanos, tal y como está redactada a 4 de marzo de 2008.

167 Bob Watt, *Implementing Electronic Voting, A report Addressing The Legal Issues Raised By The Implementation Of Electronic Voting*, marzo de 2002, disponible online en http://www.dca.gov.uk/elections/e-voting/pdf/legal-report.pdf, accedido el 7 de diciembre de 2007.

168 David de Ugarte, *El poder de las redes*, Ed. El Cobre, 2007.

169 Angel Medinilla, "El abuso de las tarjetas de fidelización",

El blog salmón, 24 de diciembre de 2007, disponible online en http://www.elblogsalmon.com/2007/12/24-el-abuso-de-las-tarjetas-de-fidelizacion, accedido el 16 de febrero de 2008.

170John Perry Barlow, *Declaración de independencia del ciberespacio*, 8 de febrero de 1996, disponible online en http://biblioweb.sindominio.net/telematica/manif_barlow.html, accedido el 14 de abril de 2008.