Privacidad y libertad de expresión en el ámbito de las TIC

Carlos García-Saura. *Escuela Politécnica Superior, Univ. Autónoma de Madrid.*

Abril 2014 - www.carlosgs.es

Desde la revolución industrial, la sociedad está en constante cambio. La aparición de las TIC y la red global Internet han acelerado este cambio hasta convertirlo en un desafío para el Derecho tradicional. Los vacíos legales existentes debido al desconocimiento de la moderna tecnología por parte de la normativa, suponen la aparición de nuevas dimensiones para la injusticia ¿Es posible que se estén viendo afectados los derechos básicos, tales como la Libertad de Expresión o el Derecho al Olvido? Se analizan tanto las implicaciones de un Estado que desconoce las realidades de las nuevas tecnologías así como, en el otro extremo, las posibles consecuencias de la implantación de un Estado tecnocrático. Se revisa además otro dilema moral: La negociabilidad de la información personal en contraste con la Privacidad por Defecto, y la fuerte componente económica característica de las Redes Sociales. Finalmente se trata de dar respuesta a la cuestión ¿Hasta qué punto está preparada la sociedad para hacer frente a las nuevas realidades tecnológicas?

Palabras clave: *Internet, e-privacidad, libre expresión, tecnocracia, Redes Sociales, Personal Information Management, Data mining, Big-Data, cibercrimen*

1. Introducción

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC) posterior a la revolución industrial ha supuesto cambios drásticos en la estructura fundamental de la sociedad. Con la aparición y globalización de la red Internet se debe hacer frente a nuevos paradigmas sin precedentes en torno a derechos fundamentales como la libertad de expresión [Boorstin, 2013] y la privacidad [Sola-Martínez, 2009].

La red ha supuesto una revolución incuestionable, y su amplia presencia como plataforma TIC se ve reflejada en su constante aparición en los medios informativos (ej. *los escándalos de privacidad por espionajes del gobierno, la recopilación de meta-datos y el Big-Data, la detección de vulnerabilidades en los sistemas de encriptación y comunicaciones seguras -SSL-... etc.*). Internet y las Redes Sociales ya forman parte de la vida diaria de una gran parte de la población, por lo que es necesario considerar hasta qué punto se están poniendo en riesgo tanto la difusión de la información personal [Roig, 2009] como la garantía de los derechos fundamentales como la Libre Expresión [Cotino-Hueso, 2007] o el Derecho al Olvido [Davara-Rodríguez, 2013a].

Se van a analizar aspectos que resultan especialmente críticos, como son las expectativas que se deben tener en relación con la privacidad y derechos de las personas en Internet, el dilema legal en torno al plagio y gestión digital de derechos (DRM) [Cotino-Hueso, 2011], la influencia política y el ejercicio del poder a través de las TIC [Stallman, 1984, Falk, 1997], y el fomento de la libre expresión a través de las licencias abiertas y plataformas *on-line* [Ozer and Conley, 2012].

También se estudiarán los efectos del rápido avance de la técnica, como desafío para el Derecho tradicional. La obsolescencia legislativa [Díez-Picazo, 1979] abre la posibilidad de injusticia en la censura, y el elevado riesgo de atentado contra los derechos fundamentales [Buxó i Rey, 2004] motiva el análisis de una legislación más adecuada. Se consideran además los nuevos retos administrativos de un concepto tan social, etéreo y subjetivo como es la privacidad [Serwin and Stow, 2012]. En relación con la fuerte componente económica característica de las Redes Sociales se contrasta además la negociabilidad de la información personal con la Privacidad por Defecto.

Por último se dará una visión conjunta para determinar hasta qué punto está preparada la sociedad para hacer frente a las nuevas realidades tecnológicas.

2. Privacidad y libertad de expresión

Las TIC e Internet proporcionan un espacio intercultural global sin precedentes [Boorstin, 2013], en el que compartir ideas y así evolucionar como sociedad. El aspecto positivo de dichas infraestructuras es indiscutible: las personas ya no se ven limitadas por los retardos característicos de los sistemas de comunicación tradicionales. Además las nuevas tecnologías han conseguido reducir el coste de las interacciones a distancia [Falk, 1997, Pifarré, 2013]. Actualmente es incluso posible considerar Internet y las Redes Sociales como un instrumento a través del cual ejercer los derechos y libertades fundamentales [Cotino-Hueso, 2007], por ejemplo dentro del contexto del asociacionismo y coordinación del activismo mediante la Red.

No obstante, la masificación social está suponiendo nuevas realidades en cuanto a la gestión de estas libertades individuales, llegando a poner en entredicho incluso la misma garantía de los derechos fundamentales [Roig, 2010]. De este modo, es necesario reconocer que junto con la explosión de las TIC han ido apareciendo ciertos "riesgos tecnológicos" asociados, cuya magnitud es importante cuantificar.

2.1. Efectos sociales de las nuevas tecnologías

El desarrollo tecnológico se encuentra íntimamente ligado al cambio social. Por ejemplo, respecto a la gestión de la información personal, ésta era tradicionalmente llevada a cabo por cada individuo gracias a su memoria y a la ayuda de libros o agendas, pero desde 1950 y gracias a los ordenadores han aparecido nuevos métodos. Se trata de las PIM (*Personal Information Management*), que han desatado un cambio dramático en la forma en que se interacciona con éstos datos [Jones, 2007] al ofrecer numerosos beneficios: no sólo ayudan a suplir los problemas de memoria de las personas, sino que mejoran la educación gracias a la personalización y adaptación, aumentan la productividad en las empresas [Ozer and Conley, 2012], facilitan a la gente con discapacidad el llevar una vida normal... etc. Un ejemplo a destacar es el correo electrónico o *e-mail*, que al poco tiempo de su invención pasó de ser utilizado únicamente para mensajería, para servir como un sistema de gestión de tareas, documentos y contactos personales.

Junto con las TIC, no es posible concebir la sociedad actual -ni futura- sin la presencia de las PIM o métodos de manejo de la Información Personal. Aún así, las PIM tienen un carácter multidisciplinar y su análisis es complejo, siendo los resultados de sus efectos visibles sólo a largo plazo. Además, con el auge de las actividades *on-line* han aparecido nuevos riesgos en cuanto a la protección

de la intimidad y los datos personales [Davara-Rodríguez, 2013a], existiendo la posibilidad de que los datos escapen al ámbito de control del titular y sean analizados o explotados por fuentes ajenas y sin consentimiento. Es por ello que la importancia del análisis de las PIM crece constantemente.

Otros ejemplos de interés son los servicios "en la nube" como las Redes Sociales o el *cloud computing* [Sola-Martínez, 2009]. Aunque ambos son servicios en la nube, es importante destacar las diferencias entre los dos sistemas: las Redes Sociales son plataformas en red donde las personas pueden interaccionar y compartir experiencias, mientras que el *cloud computing* engloba los servicios que proporcionan la capacidad de operar con información almacenada en la *nube de datos*. El efecto de las TIC en la sociedad actual es indiscutible, siendo éstos ejemplos un claro reflejo del cambio en los hábitos fundamentales de las personas.

2.2. Los riesgos de la sobre-conectividad

La gran aceptación social de las nuevas tecnologías ha provocado que actualmente sean omnipresentes en todos los ámbitos de la vida diaria. Los claros beneficios de las nuevas tecnologías han fomentado su integración, pero hacen que en ocasiones se desestime su posible impacto negativo. Entre las nuevas aplicaciones de la tecnología se encuentra un amplio abanico de sistemas, cuyos riesgos es preciso analizar:

- *En las comunicaciones:* Desde la aparición de los sistemas de comunicación a distancia, como la telefonía, ha existido siempre mucha polémica en torno a la privacidad en las comunicaciones [Falk, 1997]. Muchos operadores han sido criticados por sus actividades de recolección de datos, pero se excusan en que solamente se trata de información relativa al servicio que proporcionan y en que lo único que almacenan son *meta-datos* (es decir, información fragmentada que no puede ser asociada con una determinada persona). Los nuevos servicios en red como *la web, los buscadores o las Redes Sociales*, también han utilizado esta excusa para hacer uso de las *cookies* (un tipo de meta-dato que se utiliza en los navegadores web). Pero la ética de dichas prácticas se ve cuestionada cuando los meta-datos recopilados, en principio anónimos, son procesados en conjunto con otras grandes bases de datos [Sola-Martínez, 2009], lo que puede hacer posible asociar a una persona con la información "anónima" que generó.

- *En los contenidos multimedia y el ocio:* La extensión en el uso de la televisión por cable y el desarrollo del *vídeo bajo demanda* también ha

creado problemas en relación a los meta-datos, haciendo que varios países hayan establecido una regulación. Por ejemplo, en Estados Unidos las compañías proveedoras de servicios de televisión por cable deben informar a los usuarios de cuál es la información que recogen y con qué propósito [Falk, 1997]. Con el cambio en la forma de consumo de los contenidos audiovisuales y la aparición multitud de servicios *on-line* dedicados al ocio, es imprescindible mantenerse alerta ante éstas posibles violaciones de la intimidad.

- *En la identificación y acceso:* Las nuevas técnicas de identificación y firma electrónica resultan ya una parte esencial de la interacción digital. El desarrollo de las tarjetas de crédito electrónicas aceleró las transacciones [García-Solé, 1998] y ha permitido que se desarrolle el comercio *on-line*, pero a pesar de las grandes ventajas de estos sistemas, de nuevo se presenta el riesgo de que los derechos se vean afectados. Podría darse, por ejemplo, un traspaso no consentido de la información fiscal de un cliente a terceros. Es necesario por tanto regular la información que recopilan las entidades financieras y el uso que le dan [Falk, 1997]. Por otra parte están los nuevos métodos de identificación como el etiquetado RFID o NFC (*Near Field Communication*, chips con dispositivos inductivos que operan a la frecuencia $13{,}56MHz$), que se están implantando en los últimos años. Dichos dispositivos proveen identificadores únicos que pueden ser leídos de forma remota por cualquiera que disponga de un receptor adecuado [Davara-Rodríguez, 2013b]. Existe por tanto el riesgo de que se utilicen éstos códigos de radiofrecuencia, presentes en el etiquetado de los productos, para conocer los hábitos de consumo de una persona sin su consentimiento previo.

- *En la automatización de tareas:* También han surgido nuevos conceptos tecnológicos relativos a la *domótica* o gestión automatizada del hogar, siendo común ver sistemas de ahorro energético y confort como la regulación automática de luz y calefacción, robots de limpieza, nuevos sistemas de detección de intrusiones y alarma... etc. El *"Internet de las Cosas"* busca llevar la domótica un paso más allá [Roig, 2009], dotando de conectividad a un número mucho más elevado de aparatos para su gestión a través de Internet. En vista de un futuro en el que todos los objetos podrán interaccionar con las personas en su entorno y ser accedidos desde la red, se plantean numerosas cuestiones éticas que deberán ser resueltas: ¿Serán seguros? ¿Cómo se afrontarán entonces las potenciales intrusiones de la privacidad?

- *En las aplicaciones móviles:* La amplia difusión de los teléfonos móviles inteligentes o *smartphones* se debe en parte a la gran utilidad de las aplicaciones móviles, que permiten solucionar de forma rápida muchos problemas de la vida cotidiana. Por ejemplo, las aplicaciones de orientación como *Google Maps* permiten planificar los desplazamientos de forma eficiente, y las aplicaciones sociales como *Telegram* ofrecen servicios de comunicación sencillos de usar. Pero de nuevo existen riesgos relacionados a la recolección y explotación no consentida de los datos personales. Por ejemplo, la *geolocalización* (conocimiento de la posición de un dispositivo) puede permitir el seguimiento de una persona a través de su terminal. Un estudio de *Pew Internet & American Life Project* [Boyles et al., 2012] mostró que más de la mitad de usuarios de terminales móviles ha desinstalado o decidido no instalar alguna aplicación debido a preocupaciones por la seguridad de su información personal, lo que ilustra que existe una cierta conciencia social al respecto de las garantías de las aplicaciones móviles.

En un mundo cada vez más conectado a Internet, se ha visto que el progreso trae consigo nuevos riesgos relacionados con la gestión de la información personal y la garantía del derecho a la intimidad. El progreso como sociedad debería estar siempre regido por la ética y el análisis crítico, pero dado que las TIC pueden estar ejerciendo control sobre la forma de pensar de las personas [Jones, 2007], se hace frente a un problema de gran magnitud que pone en cuestión si la sociedad está realmente preparada para hacer frente a las nuevas realidades tecnológicas.

2.3. La gestión moderna del poder: Hacia una sociedad tecnocrática

Con la amplia presencia en los medios de términos tan actuales como el *big-data* o el *data mining* -relacionados con la recolección y procesado masivo de datos respectivamente- resulta intranquilizador conocer el riesgo que éstos suponen para la garantía de los derechos fundamentales [Sola-Martínez, 2009]. Es más, la presencia de un estado y organismos cada vez más conscientes de la gran influencia que aporta tener el control sobre los datos de los ciudadanos, y dado el enorme grado de analfabetismo tecnológico, es preocupante el hecho de que las TIC ya sean un pilar fundamental de la sociedad.

Otro hecho que también motiva dicha preocupación es el rol de los medios de comunicación como potencial inhibidor de las libertades básicas de información, expresión o libre albedrío [Cotino-Hueso, 2011]. A ésto se suma la falta de

precisión en las traducciones al trasladar los conceptos entre culturas, que se ve acentuada en especial al tratar las razones que relacionan lo tecnológico y lo social [Buxó i Rey, 2004].

La desinformación individual respecto de las TIC supone un riesgo para la sociedad en su conjunto. Basta citar la política de gestión de datos en multitud de plataformas *on-line*. Éstas suelen basar su política de privacidad en unas normas y términos de uso que cada usuario debe aceptar en el momento del registro; Sin embargo, la mayoría de personas desconoce las implicaciones de dichas condiciones y las acepta sin siquiera leerlas, quedando sus datos a merced del organismo proveedor del servicio [Sola-Martínez, 2009].

Para entender mejor las circunstancias que motivan estos "traspasos de poder" que se producen entre los usuarios y las empresas, se va a analizar cual es la dimensión actual del concepto del *poder*. Se ha acudido a las definiciones clásicas, en este caso las *48 Leyes del Poder* recopiladas por Robert Greene [Greene, 2000], para ver su proyección en el contexto de Internet.

- *Ley 40: "Desdeñar la comida gratuita"* Dada la inmensa cantidad de servicios web gratuitos, es necesario plantearse cómo obtienen los beneficios. Si se leen detenidamente los términos de uso es común identificar que los proveedores pueden comerciar con los datos personales que se les proporciona. Cuando una persona utiliza éstos servicios les otorga entonces un poder, muchas veces absoluto, sobre sus datos.

- *Leyes 14, 32 y 33: "Actuar como un amigo, trabajar como un espía", "Jugar con las fantasías de la gente", y "Descubrir el talón de aquiles de cada persona"* Una entidad puede ofrecer un servicio de éxito mostrándose abierta y atractiva a los usuarios, siendo su objetivo real amasar grandes cantidades de información relativa a ellos. Conociendo detalles sobre la forma de ser y los hábitos de cada individuo es posible entonces la personalización y adecuación a sus necesidades -e incluso debilidades- ofreciendo una experiencia cada vez más alienante. Así, la entidad puede conseguir progresivamente un poder empático, y el control sobre las decisiones y acciones de sus usuarios.

- *Leyes 31 y 43: "Controlar las opciones, conseguir que los demás jueguen con nuestras cartas" y "Manipular los corazones y las mentes de los demás"* Las grandes empresas tecnológicas -que ya disponen de una amplia base de usuarios- tienen el poder de determinar qué productos u opciones mantiene y cuales deja de ofrecer. De este modo se tiene un control directo sobre las opciones, pudiendo manipular entonces las decisiones de los usuarios frente a un determinado producto. Google, por ejemplo,

> dispone de un gran abanico de servicios y se ha visto que cada cierto tiempo elimina los que menos le convienen. Uno de ellos fue *Google Reader*, con su cierre en 2013 la empresa trató de promocionar el uso de su red social *Google+*.

Como puede verse, las bases del poder moderno se encuentran en la falta de conocimiento técnico por parte de la mayoría de las personas, que les impide detectar cuándo se están produciendo recortes en su libertades de pensamiento o de acción. De este modo, se le otorga al poder mediático la capacidad de confirmar o desconfirmar la realidad de cualquier faceta de las TIC [Buxó i Rey, 2004]. Pero una sociedad democrática se basa en que los ciudadanos tengan una serie de derechos y garantías ante la información para poder hacer decisiones en base a su propio juicio.

Los efectos sobre la libertad de juicio generan entonces el riesgo de que las tecnologías sean utilizadas como mecanismo de influencia política, lo que se resume muy bien con la siguiente cita de Miguel Ángel Davara:

> *"Las TIC y los responsables de su definición, en un mercado laboral y económico y en una situación social angustiosa, empiezan a tener la última palabra" [Davara-Rodríguez, 2013b]*

El poder de unos pocos en base a la influencia de la tecnología supone el establecimiento gradual de una sociedad tecnocrática. Ante esta situación, es necesario buscar nuevas formas de evitar la vulneración de los derechos básicos para mantener una democracia real y evitar las injusticias.

2.4. Garantías tecnológicas y defensa de los derechos fundamentales

Se plantea por tanto la necesidad de la participación social para la decisión de las políticas en torno a las nuevas tecnologías, pero la falta de conocimiento técnico por parte de grandes sectores de la población inhibe el consenso en las soluciones. Un debate público eficiente necesita contemplar la colaboración entre equipos de expertos multidisciplinarios y los grupos locales representativos y agencias públicas [Buxó i Rey, 2004]. De este modo se podría llevar un seguimiento imparcial de los procesos de implementación, y conseguir así que todos los ciudadanos conozcan los problemas inherentes a las TIC para poder contrastar y confrontar los intereses, opiniones e información de los medios de comunicación.

No obstante, la privacidad sigue siendo un concepto muy subjetivo y su definición es compleja dentro del contexto actual[1]. Por ello es necesaria la implantación de una protección tecnológica desde el mismo momento de diseño de un sistema; los derechos fundamentales no pueden quedar reducidos a una opción "activable" [Roig, 2009]. De aquí surge el concepto de la Privacidad desde el Diseño o *privacidad por defecto*, en inglés *"Privacy by Design"* (PbD) [Roig, 2010, Serwin and Stow, 2012, Davara-Rodríguez, 2013b].

Los sistemas de administración por vía electrónica (*e-administración*) han supuesto una aceleración respecto a los sistemas tradicionales, y son posibles gracias al desarrollo de los medios de comercio electrónico [García-Solé, 1998] así como de las *Privacy Enhancing Technologies* (PET) o tecnologías protectoras de la privacidad como son la firma o el cifrado digital [Roig, 2009, Roig, 2010]. La seguridad y la protección de la intimidad que proporcionan dichos sistemas tienen su base en robustos algoritmos matemáticos cuya implementación dista de ser trivial. Surge el riesgo de la implantación en el software de "puertas traseras" o *backdoors* que permitan a un tercero obtener control sobre los datos protegidos, por lo que resulta esencial llevar un análisis minucioso a nivel técnico de este tipo de tecnologías que ofrezca ciertas garantías.

Pensadores como Richard M. Stallman ya previeron, en vista de que el software empezaba a ocupar posiciones críticas en el funcionamiento de la sociedad, que cuando un usuario no tiene control sobre las TIC son éstas las que pueden controlarle a él, lo que las convierte en un instrumento injusto de poder [Stallman, 1984]. Para evitar ésta situación, las licencias abiertas propuestas inicialmente por Stallman con el proyecto *GNU* definieron las libertades fundamentales que debe ofrecer un software para dar el poder a los usuarios: éstos deben poder *utilizar, copiar, distribuir, y estudiar el software para poder modificarlo y adecuarlo a sus necesidades.*

Otros autores también coinciden en que las licencias abiertas no sólo facilitan y protegen la libertad de expresión, sino que también pueden promover la transparencia política [Sola-Martínez, 2009, Cotino-Hueso, 2011]. Un gobierno que permitiese conocer la implementación de un determinado sistema de votación estaría poniéndolo bajo la luz pública y fomentando así la transparencia política a través de las TIC.

Por otra parte, la libertad en las licencias de contenidos choca directamente con el derecho de propiedad intelectual [Falk, 1997, Cotino-Hueso, 2011]. Aunque la tecnología ha proporcionado las técnicas de identificación y ofuscación

[1] Una posible definición: *"La privacidad es la válvula de seguridad que la sociedad impone al uso y compartición de datos. Está influenciada por el avance tecnológico, así como los puntos de vista sociales respecto de la información." [Serwin and Stow, 2012]*

necesarias para implantar los sistemas de gestión del derecho de contenido digital (*Digital Rights Management* -DRM-), éstas vienen servidas de polémica [Roig, 2010]. Previamente a la invención del comercio digital, siempre había sido posible compartir los contenidos audiovisuales como *libros, música o vídeo* de forma completamente anónima. Pero con la llegada de los contenidos digitales y su capacidad de copia y difusión a través de la red, el DRM está tratando de limitar éstas prácticas. Las técnicas empleadas se basan en la restricción del anonimato en las ventas, con la firma digital individualizada de los contenidos. Se trata de nuevo de unos mecanismos capaces de ejercer un poder sobre los usuarios, en este caso, de los servicios de descarga o *streaming* de contenido multimedia digital.

Además de una protección tecnológica, también es necesario que se fomente la educación multimodal de la ciudadanía para conseguir crear una conciencia global respecto de las TIC [Buxó i Rey, 2004, Sola-Martínez, 2009]. Como se ha visto, los servicios web y Redes Sociales deben ser utilizadas con cautela, por lo que es necesario formar a los usuarios en un manejo responsable de Internet. En el futuro será esencial que la sociedad esté bien concienciada para la detección precoz de las malas prácticas y así se denuncien los recortes en el ámbito de la libertad de expresión y de la privacidad.

2.5. Problemática legal asociada a las TIC

Los avances en la técnica respecto a la gestión de datos personales han supuesto nuevas realidades que entran en conflicto con la legislación vigente, incrementando los riesgos de que se produzca obsolescencia legislativa, y por tanto se produzcan decisiones administrativas erróneas. Es más, el marco regulador sigue siendo inexistente o muy limitado [Roig, 2009, Davara-Rodríguez, 2013b] y el sistema legal todavía se basa en leyes obsoletas que fueron definidas en un contexto social muy distinto al actual. Esto supone que, en general, los nuevos conflictos se tienen que resolver por vía interpretativa, a veces forzando la norma.

Ante la posibilidad de que produzcan atentados contra los derechos fundamentales se ha puesto en evidencia la necesidad de afrontar este dilema legislativo desde un punto de vista multidisciplinar [Buxó i Rey, 2004], admitiendo de este modo que hoy en día la tecnología y los derechos fundamentales están intrínsecamente relacionados [Roig, 2010]. Así, en lugar de separar las TIC de los derechos y libertades, resulta mucho más efectivo el trato en su conjunto mediante el enriquecedor diálogo entre juristas e ingenieros (*"IT Law"* o *"IT for Lawyers"*). Pero en la práctica dicho concepto aún necesita un tiempo para llegar a funcionar de manera eficiente. Algunos autores [Pifarré, 2013] muestran

que la reacción más común del derecho ante las nuevas realidades sigue siendo la tipificación de los delitos informáticos (ej. los *"hacker"* o atacantes, como término genérico).

De todos modos la ley existente sigue siendo aplicable en la mayoría de los supuestos [Miró-Llinares, 2013]. Por ejemplo, ante delitos como el ciberacoso, o ataques contra derechos individuales (el honor, la libertad, la intimidad o la propia dignidad personal) se suelen aplicar tipos legales existentes, al ser calificados como amenazas, coacciones, injurias... etc. También es importante resaltar que la ley ha demostrado ser contundente en determinados aspectos del *cibercrimen* como son el terrorismo, el comercio ilegal, la difusión de contenidos obscenos como la pornografía infantil, o incluso la difamación [Falk, 1997], a pesar de las dificultades técnicas para encajar en su regulación.

Los verdaderos problemas salen a la luz cuando se admite que es simplemente imposible regular todas y cada una de las posibles conductas y situaciones que se van dando en Internet. Por ejemplo, la amplia presencia e integración de las infraestructuras electrónicas en la sociedad (ej. *servidores de información, teléfonos móviles, smartphones, dispositivos USB, CD-Rom, DVD, reproductores de música... etc.*) hace que muchas veces sea imprescindible el acceso a éstas para el análisis del crimen. Pero el acceso a la información almacenada en los dispositivos electrónicos tiene el potencial de afectar a varios derechos fundamentales reflejados en la Constitución Española [Delgado-Martín, 2013] como son el derecho a la intimidad personal (art. 18.1 CE), el derecho al secreto de las comunicaciones (art. 18.3 CE), el derecho de autodeterminación informativa en el ámbito de la protección de datos personales (art. 18.4 CE), y en el caso de que un dispositivo se encuentre durante una entrada y registro domiciliario, incluso puede verse afectado el derecho a la inviolabilidad domiciliaria (art. 18.2 CE).

Otro de los principales problemas se encuentra entre las características básicas de las Tecnologías de la Información; Aunque la historia ha mostrado que los medios de almacenamiento a largo plazo -como los libros-, lejos de suponer un riesgo han sido incluso un aliciente para la garantía de los derechos fundamentales, las TIC se presentan como una realidad más compleja. Su capacidad de procesado de datos es mucho más elevada, y éstos medios digitales tienen el potencial de "no olvidar" la información que circula a través de ellos, pudiendo por el contrario registrar y almacenar esos datos de forma indefinida. Esto implica que la actividad en la Red queda siempre registrada, o por menos deja una huella que puede seguir siendo identificable tras muchos años. Es en este nuevo contexto tecnológico donde surge la definición del *"Derecho al Olvido en Internet: Aquel derecho que tiene el titular de un dato a que éste sea borrado o bloqueado, cuando se produzcan determinadas circunstancias y, en particular,*

que no sea accesible a través de la red Internet" [Davara-Rodríguez, 2013a][2]. En la práctica resulta muy difícil garantizar este derecho dada la imposibilidad de abarcar todo rastro en las redes de comunicaciones; Una información puede ser accedida, por ejemplo, por *buscadores on-line* alejados del control de los responsables del fichero o tratamiento que lo acogía, saliendo de este modo los datos involuntariamente de su ámbito de responsabilidad y dejando vulnerable al titular del dato.

Todo lo expuesto indica que es necesaria una mayor flexibilidad de las reglas para permitir su adaptación al constante cambio [Boorstin, 2013] pero conservando al mismo tiempo los principios básicos, y ésto puede conseguirse gracias a la colaboración multidisciplinar entre el ámbito de la tecnología y del Derecho.

2.6. Los límites de la libertad de expresión

El reto legislativo del "ciberespacio" se ve acentuado por el hecho de que tiene un ámbito global: no está asociado a ningún país en particular, y es por ello que algunos autores [Miró-Llinares, 2013] sugieren que la responsabilidad de gestión recaiga sobre la Organización de las Naciones Unidas (ONU). Aún así, ya se ha visto que la gestión del poder es un tema que genera debate en torno a la gran responsabilidad asociada una asignación incorrecta del poder de decisión. Es por esto que cada país trata de resolver los problemas que les afectan en relación a la red, causando en ocasiones conflictos de intereses entre las múltiples circunscripciones legales presentes en Internet. Así, la asignación de poderes respecto al control de la Red es un tema que parece estar lejos de ser resuelto.

Quien disponga del poder de imponer dichas leyes podría ejercer control sobre la libertad de expresión, y los límites que se establezcan serán decisivos de cara a una sociedad democrática [Boorstin, 2013]. Por ejemplo, se podría excusar una decisión legal de censura dados los problemas relativos al riesgo de los menores en Internet y su privacidad. Una censura de la web implicaría recortar en derechos como la libertad de expresión ¿es ésto necesario? La posible solución para evitar este retroceso podría ser la correcta tutela de los menores en el manejo de las nuevas tecnologías.

Otro ejemplo se encuentra en el ámbito de la piratería y el plagio. Si bien es cierto que las TIC -especialmente Internet- son atractivas en gran medida

[2] Otra definición: *"Derecho de los interesados a que se cese en el tratamiento y se supriman o cancelen los datos cuando no sean necesarios para los fines legítimos para los que se hubieran obtenido, o sencillamente cuando así sea la voluntad del titular de los datos"* [Davara-Rodríguez, 2013a]

por la facilidad que proporcionan para recolectar y transmitir información con gran fidelidad, esto supone otra gran problemática añadida de cara a asegurar los derechos de propiedad intelectual [Cotino-Hueso, 2011] ¿Cómo se puede conseguir que la web sea abierta y libre, evitando a su vez el plagio y la piratería?. La principal solución que se está empleando es el *Digital Rights Management (DRM)*, pero ya se ha visto que trae consigo bastantes problemas relativos a la privacidad, que generan a su vez más conflictos en torno a la gestión de los derechos de autor.

Además, desde la aparición de Internet se ha producido una tendencia constante a la restricción del anonimato [Roig, 2010], que afecta al derecho a la información por cualquiera. Ésto se ve presente en la desaparición de servicios como el correo electrónico anónimo, comentarios anónimos en los foros públicos de debate, o incluso la navegación anónima por Internet. Las principales excusas que se ponen para justificar éstas restricciones están siendo los problemas legales derivados de la gestión del anonimato en la red, incluyendo por ejemplo el problema del ciberacoso.

Ha quedado claro que las respuestas que vaya dando el Derecho pueden ser decisivas [Cotino-Hueso, 2007] y condicionarán el alcance y posibilidades de las TIC en el futuro. Por ello, en un entorno perfecto para la creación de leyes que limiten las libertades básicas, es ahora más que nunca cuando se debe permanecer en alerta para detectar y denunciar las posibles injusticias legales.

2.7. Aspectos económicos: El negocio de los datos

Dejando de lado sus ámbitos social y legislativo, la privacidad y la libertad de expresión tienen una amplia proyección económica que no se puede ignorar. En primer lugar hay que considerar el hecho de que multitud de empresas -y no solamente los proveedores de servicios *on-line*- tienen el control sobre ingentes cantidades de datos relacionados con muy diversos aspectos personales de los usuarios. Cada empresa puede disponer, en general, de segmentos limitados de información en torno a sus clientes, de modo que se tiene un conocimiento fragmentado. El siguiente ejemplo ilustra ésta circunstancia: en el caso de un centro comercial es posible que éste disponga del registro de compras realizadas con una determinada tarjeta de crédito [García-Solé, 1998], mientras que una red social como Facebook puede conocer las amistades y conexiones familiares de una persona. En este sentido, Facebook podría querer adquirir a través de un centro comercial información relativa a las preferencias de compra de sus usuarios. Pero ¿qué es lo que motiva a las empresas a amasar tal cantidad de información?

El interés comercial más claro se encuentra en el ámbito de la publicidad

a la hora de ofrecer un determinado producto o servicio. Los analistas de marketing coinciden en la importancia de adaptar las características de la publicidad para armonizar mejor con los ideales y necesidades de los sectores a los que está destinada. Resulta cuanto menos sorprendente el hecho de que una publicidad bien adaptada puede ser decisiva en relación al éxito o fracaso de la entrada de un determinado producto en el mercado. Con la llegada de las TIC y el tratamiento masivo de datos, se ha visto que esta adaptabilidad de la publicidad puede dejar de enfocarse a diferentes sectores y escalar hasta convertirse en publicidad individualizada, personalizada hacia cada usuario [Roig, 2009]. De este modo se puede conseguir despertar reacciones emocionales en los potenciales clientes, consiguiendo mejorar aún más las ventas y con ello los resultados comerciales. Por tanto, se puede concluir que lo que motiva a las empresas a recopilar grandes cantidades de datos es la potencial repercusión económica asociada a un mejor conocimiento de sus usuarios.

Cuando se da una circunstancia como ésta, donde se observa un potencial beneficio económico, se debe considerar que también se pueden producir grandes pérdidas. Hay que tener en cuenta cuales son los riesgos que pueden provocar reacciones opuestas a las esperadas: por ejemplo, una personalización excesiva de la publicidad puede llegar incluso a originar rechazo por parte de los usuarios al percibir éstos una intrusión de su privacidad. Un buen caso de ejemplo es Facebook y su sistema *Beacon*, lanzado en noviembre de 2007. Dicho sistema tenía como objetivo llevar un registro de las compras *on-line* realizadas por cada usuario, y compartirlas de forma automática con el resto de sus contactos. Tan sólo un mes después de implementar dicho sistema, Facebook ya había recibido numerosas quejas de usuarios que habían comprado regalos para las fiestas navideñas y vieron estropeadas las sorpresas en forma de detallados mensajes públicos mostrando todas sus compras [Nakashiwa, 2007]. La empresa trató de solventar este problema añadiendo una opción clara para deshabilitar el servicio *Beacon* al momento de realizar las compras, lo que provocó la dramática caída en su uso debido a la controversia creada, culminando con el cierre del servicio en septiembre de 2009. El mismo CEO de Facebook, Mark Zuckerberg, calificaría más tarde a *Beacon* como "un error", dado el desprestigio y rechazo social ocasionado a la compañía.

Beacon fracasó por una incorrecta gestión de la privacidad de los usuarios, que percibieron no sólo una intrusión por parte de Facebook en los datos de sus compras personales, sino que además vieron utilizada su información de la peor forma posible ¡en su contra! La percepción del uso de los datos personales propios supone grandes efectos en la aceptación de la publicidad personalizada. Un estudio realizado por el NEI Institute [Tucker, 2011] cuantificó dichos efectos, comprobando que tras implementar un control avanzado de la privacidad los

usuarios tenían el doble de probabilidad de hacer *click* en los anuncios dirigidos, mostrando así que es decisivo que las personas perciban un control adecuado de su información personal.

Ésto se ve más claro en el contexto de las buenas prácticas en el mundo empresarial: La satisfacción de los usuarios tiene una proyección positiva en los beneficios, y se consigue gracias a una gestión correcta de su privacidad y mediante el fomento de su libre expresión [Ozer and Conley, 2012]. Ya se han visto los principales puntos a tener en cuenta de cara a la gestión de la privacidad: el respeto y seguridad de los datos, la transparencia, así como la Privacidad desde el Diseño (PbD) para dar el control a los usuarios. En cuanto a la libertad de expresión, las buenas prácticas incluyen además: el fomento del libre diálogo entre los usuarios, la cautela en la moderación evitando la censura, la correcta protección del anonimato en la identidad, y finalmente la promoción de la creatividad dejando que los usuarios decidan cómo usar un producto y establezcan opiniones sobre él.

3. A modo de conclusión

Se ha realizado un análisis relativo a la privacidad y la libertad de expresión, en el ámbito de la plataforma intercultural sin precedentes que son Internet y las TIC. Aspectos positivos tales como la reducción de tiempo y coste en las interacciones, y su función como herramienta para ejercer los derechos y libertades fundamentales en foros públicos de debate -como las Redes Sociales-, se han visto contrastados con los problemas relativos a la masificación y cambio social ligados al desarrollo tecnológico. Y es que la omnipresencia de las TIC puede estar afectando a la forma de pensar de las personas. La aparición de nuevos sistemas de gestión de la información personal (*Personal Information Management* ó PIM), como el correo electrónico o el *cloud computing*, han mejorado la calidad de vida de las personas pero a su vez comportan "riesgos tecnológicos" asociados a la sobre-conectividad de una sociedad cada vez más dependiente de Internet.

Los riesgos en cuanto a la privacidad y gestión de datos personales son claros, existiendo la posibilidad de que una información escape del ámbito de control del titular y sea analizada o explotada sin su consentimiento. La enorme capacidad de procesado de las nuevas técnicas de recolección y tratado masivo de datos (*big-data* o *data mining*) suponen amenazas para la privacidad nunca antes vistas. En el caso de las comunicaciones o el ocio multimedia, se ha visto que la recolección de *meta-datos* y el uso de *cookies* pueden suponer violaciones de la intimidad al tratarse de datos que pueden llegar a ser identificables con una

determinada persona. En cuanto a la identificación y el acceso, surgen problemas relativos al firmado electrónico y cifrado de documentos -los algoritmos pueden ser seguros pero las implementaciones vulnerables-, así como el riesgo de que se utilicen identificadores por radiofrecuencia (etiquetado RFID ó NFC) para conocer los hábitos de consumo de una persona. La domótica y el *"Internet de las Cosas"*, en constante implantación, suponen nuevas posibilidades de intrusión de la privacidad que han cuestionado su seguridad. En las aplicaciones móviles, problemas como la *geolocalización* para el seguimiento de personas han despertado la preocupación de los usuarios de los dispositivos.

Los riesgos en torno a la libertad de expresión tienen su base en la enajenación de derechos fundamentales por medio de las TIC, que ha mostrado no ser más que el reflejo de las definiciones tradicionales del *poder*. Éstas tienen una validez renovada en el contexto de Internet: El poder económico de una entidad, conseguido mediante la oferta gratuita de sus productos con la intención de obtener una base de usuarios; el poder empático derivado de una personalización y adaptación de los servicios; y finalmente el poder tecnológico de las grandes empresas como Google, capaces de controlar las opciones y determinar qué productos se mantienen. La lucha contra el cibercrimen también está suponiendo recortes en los derechos fundamentales: la censura de la web -un ataque contra la libertad de expresión-, la tendencia constante a la restricción del anonimato (con la desaparición de servicios como la navegación anónima, y el correo electrónico o comentarios anónimos), y las técnicas de firmado digital de la propiedad intelectual (DRM), son algunos ejemplos.

Se ha visto también que las nuevas formas de influencia en base a las TIC, sobre una población con un alto grado de analfabetismo tecnológico a la que los medios pueden confirmar o desmentir las nuevas realidades, hacen necesario el análisis de las implicaciones éticas de la deriva de la sociedad hacia un estado tecnocrático. Frente al posible uso injusto de la tecnología como instrumento de poder, y para mantener una democracia real, surge la necesidad de la participación social en la decisión de las nuevas políticas. Pero dada la falta de conocimiento técnico de los ciudadanos, así como las imprecisiones en las traducciones al tratar de trasladar conceptos tecnológicos entre diversas culturas, se plantea la colaboración multidisciplinar entre equipos de expertos.

La obsolescencia de la normativa, debida a los retos legales y técnicos que suponen las TIC, se muestra también como una amenaza contra los derechos fundamentales. Como ejemplos se han visto las incertidumbres causadas por la tipificación de los delitos informáticos (el *hacking* como término genérico) o la violación de derechos que puede suponer el acceso a datos contenidos en dispositivos electrónicos. Además, dado que la actividad en la red puede quedar registrada de forma indefinida, se ha visto el concepto de *Derecho*

al Olvido en Internet. A pesar de las dificultades técnicas que supone su garantía, previamente es necesaria una normativa más adecuada. Puesto que las respuestas del Derecho condicionarán el alcance y posibilidades de las TIC, es necesario fomentar el diálogo entre juristas e ingenieros para conseguir una mayor flexibilidad de las reglas que permita su adaptación al constante cambio.

En cuanto a la negociabilidad de la información personal, se ha estudiado la gran proyección económica de las TIC. La necesidad de las empresas por recolectar grandes cantidades de datos relativos a sus clientes tiene su base en que la publicidad dirigida y adaptada es mucho más rentable, eficiente y escalable, y en que el conocimiento mejorado de los usuarios a través de sus datos facilita las buenas prácticas.

Respecto a la pregunta sobre si la sociedad está preparada para hacer frente a las nuevas realidades tecnológicas, se puede concluir con un cierto optimismo en vista de los grandes progresos que se están llevando a cabo: la aparición de las Tecnologías Protectoras de la Privacidad (PET) como la *Privacidad desde el Diseño*; la transparencia política apoyada por las licencias abiertas; y el análisis multidisciplinar en el Derecho. Además, la garantía de los derechos fundamentales no es contradictoria con el interés de las empresas, puesto que se ha demostrado que la correcta gestión de los derechos de los usuarios repercute en los beneficios de forma positiva. Pero no se debe perder de vista que la defensa de la libertad de expresión y la privacidad en relación con las TIC van a seguir planteando problemas a nivel global. La capacidad alienante de las tecnologías digitales las puede convertir en una herramienta injusta de poder y por tanto es necesario invertir en la formación multimodal de la ciudadanía en su uso correcto y respetuoso con una sociedad libre, capaz de exigir buenas prácticas a los gobiernos y empresas tecnológicas.

4. Agradecimientos

- A D. Juan Alberto Sigüenza, profesor de la asignatura *Ingeniería y Sociedad*, bajo la tutela de quien se ha realizado el presente estudio.
- Al personal de gestión e inventariado de las bibliotecas de Derecho así como de la Escuela Politécnica en la Universidad Autónoma de Madrid.
- A todos los autores citados, cuya labor investigadora ha sido determinante. Sus referencias se listan a continuación.

Referencias

[Boorstin, 2013] Boorstin, B. (2013). Libertad de expresión en la era digital. *Periódico Expansión*.

[Boyles et al., 2012] Boyles, J. L., Smith, A., and Madden, M. (2012). Privacy and data management on mobile devices. *Pew Internet & American Life Project*.

[Buxó i Rey, 2004] Buxó i Rey, M. J. (2004). A nuevas tecnologías, nuevas políticas: Riesgo, responsabilidad y participación: Paisajes tecnoculturales y diseño de futuros sociales. *El ayer y el hoy: lecturas de antropología política*, Vol.II:pp215–223. UNED ediciones. ISBN 84-362-4824-4.

[Cotino-Hueso, 2007] Cotino-Hueso, L. (2007). *Libertad en Internet: La Red y las Libertades de Expresión e Información*. Tirant lo Blanch. ISBN 978-84-845-6943-5 (Biblioteca UAM: D/B/45/265).

[Cotino-Hueso, 2011] Cotino-Hueso, L. (2011). *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*. Publicaciones de la Universidad de Valencia. ISBN 978-84-694-0081-4.

[Davara-Rodríguez, 2013a] Davara-Rodríguez, M. A. (2013a). El derecho al olvido en internet. *Diario Semanal La Ley*, (Nº49).

[Davara-Rodríguez, 2013b] Davara-Rodríguez, M. A. (2013b). El tratamiento de datos de carácter personal y la utilización de la tecnología: entre la ética y el derecho. *Diario Semanal La Ley*, (Nº53).

[Delgado-Martín, 2013] Delgado-Martín, J. (2013). Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos. *Diario Semanal La Ley*, (Nº62).

[Díez-Picazo, 1979] Díez-Picazo, L. (1979). *Derecho y Masificación Social. Tecnología y Derecho Privado*. Civitas Ediciones S.L. ISBN 84-7398-524-9.

[Falk, 1997] Falk, K. J. (1997). Privacy and free speech issues on the internet. *UC Berkeley online publications*. `http://courses.ischool.berkeley.edu/i206/f97/GroupH/privacy.html`.

[García-Solé, 1998] García-Solé, F. (1998). Aspectos sobre la incidencia de la tecnología en el mercado de tarjetas. *Icade: Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales*, (Nº 43):pp77–98. ISSN 1889-7045.

[Greene, 2000] Greene, R. P. (2000). *Las 48 Leyes Del Poder*. Espasa Hoy. ISBN 84-239-6637-2.

[Jones, 2007] Jones, W. P. (2007). *Keeping Found Things Found: The Study and Practice of Personal Information Management*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA. ISBN 978-01-237-0866-3 (Biblioteca UAM: INF/C7250/JON).

[Miró-Llinares, 2013] Miró-Llinares, F. (2013). Derecho penal, ciber-bullying y otras formas de acoso (no sexual) en el ciber-espacio. *IDP, Revista de Internet, Derecho y Política*, (Nº16).

[Nakashiwa, 2007] Nakashiwa, E. (2007). Feeling betrayed: Facebook users force site to honor their privacy. *Washington Post*.

[Ozer and Conley, 2012] Ozer, N. A. and Conley, C. (2012). *Privacy & free speech: it's good for business*. ACLU of Northern California, 2nd edition.

[Pifarré, 2013] Pifarré, M. J. (2013). Internet y las redes sociales: Un nuevo contexto para el delito. *IDP, Revista de Internet, Derecho y Política*, (Nº16).

[Roig, 2009] Roig, A. (2009). E-privacidad y redes sociales. *IDP, Revista de Internet, Derecho y Política*, (Nº9). UOC.

[Roig, 2010] Roig, A. (2010). *Derechos fundamentales y tecnologías de la información y de las comunicaciones (TICs)*. Cuadernos de derecho constitucional. J.M. Bosch. ISBN 978-84-769-8953-1 (Biblioteca UAM: D/B/45/285).

[Serwin and Stow, 2012] Serwin, A. and Stow, T. (2012). The eye of the beholder: Operationalizing privacy by design through the power of consumer choice. *APCO Worldwide, The Lares Institute*.

[Sola-Martínez, 2009] Sola-Martínez, M.-J. (2009). Redes sociales: Más allá de la privacidad. *El profesional de la información*, Vol.18(Nº4):pp470–474.

[Stallman, 1984] Stallman, R. M. (desde 1984). Free software definition. *Free Software Foundation, Proyecto GNU*. `http://gnu.org/philosophy/`.

[Tucker, 2011] Tucker, C. (2011). Social networks, personalized advertising and privacy controls. *NEI Institute Working Paper*, (Nº10-07).