Sociología y Tecnociencia
Revista Digital de Sociología del Sistema Tecnocientífico
ISSN: 1989 - 8487

Sociología y tecnociencia/Sociology and Technoscience.

RETOS PARA LA PRIVACIDAD EN LA ERA DIGITAL. ANÁLISIS ECONÓMICA Y FILOSÓFICO POLÍTICA DEL CAPITALISMO CONTEMPORÁNEO

CHALLENGES TO PRIVACY IN THE DIGITAL AGE. PHILOSOPHICAL AND ECONOMIC POLICY ANALYSIS OF THE CONTEMPORARY CAPITALISM

NOEMÍ MILON BELTRAN
UNIVERSIDAD DE BARCELONA
nemimilonbel@hotmail.com

Enviado: 22/12/14
Modificado: 02/03/15
Aceptado: 13/03/15

Resumen: Una condición necesaria para la globalización ha sido la transnacionalización de los intercambios y flujos de información. Este aumento exponencial de la acumulación y transmisión de datos ha sido posible gracias a las nuevas tecnologías de la información y comunicación, especialmente al fenómeno conocido como Big Data. Los riesgos para la privacidad de la información personal resultan una consecuencia directa de dos hechos: en primer lugar, la necesidad de los Estados e instituciones gubernamentales de disponer de información relativa a sus sociedades *en general*, y por otro lado, el beneficio que aporta la creciente mercantilización de este tipo de información. En este trabajo se plantea si nos encontramos ante una sinergia entre estos dos intereses, produciéndose un desequilibrio de poder creciente, con la irrupción de algunas prácticas que atentan y vulneran claramente el derecho a la privacidad reconocido por la Declaración Universal de las Naciones Unidas.

Palabras Clave: *Sociedad de la información, Big Data, Privacidad*

Abstract: A necessary condition for the globalization has been the transnationalization of information exchange and flows of information. The exponential growth of the transmission and accumulation of information has been possible due to the new information and communication technologies, specially the phenomenon known as Big Data. The risks for privacy of personal data about the individuals are a direct result of two facts: On one hand, a need of the States and governmental institutions to hold information related to their societies in general. And on the other hand, the profits generated by the commodification of this kind of information. The aim of this work is to analyze if we are facing a synergy between this two interests that has as a consequence a growing power imbalance, with the apparition of some practices that are violating the fundamental right to privacy, recognized by the Official UN Universal Declaration of Human Rights.

Keywords: Information Society, Big Data, Privacy,

"Es por esto por lo que aquellos que ponen su fe en algún inmenso fenómeno que transformará el mundo, como el triunfo final de la razón o la revolución proletaria, tienen que creer que todos los problemas morales y políticos pueden ser transformados en problemas tecnológicos".

Isaiah Berlin *Cuatro ensayos sobre la libertad* p.187

La Era de la información e Internet

En las últimas dos décadas, Internet ha sido sin duda una herramienta que ha hecho cambiar profundamente el modo de funcionamiento de las empresas, los gobiernos, pero especialmente la manera en que las personas viven y se comunican. Esta comunicación y acceso a información global, inmediata y abajo coste, ha revolucionado la economía, la sociedad e incluso la política. Si nos referimos a la "sociedad" o "era de la información", tal y cómo como la define Manel Castells en "La Era de la información", esta expresión se refiere a aquella sociedad donde la manipulación y el manejo de la información han sustituido el control y la optimización de los recursos en los procesos industriales. Sin duda la información como tal siempre ha sido importante para la vida en sociedad, pero lo que diferencia y hace característica la sociedad de la información es la capacidad, no sólo de disponer de almacenes de información propios, sino también el acceso a grandes cantidades de esta generada por el resto de agentes. Es precisamente este cambio el que hace que se den una serie de hechos que transformarán la sociedad y sus estructuras.

En concreto, la información disponible se ha multiplicado debido a tres factores, los tres ligados con el adelanto de las nuevas tecnologías de la información e internet: el aumento de la velocidad de la transmisión de la información, el aumento de la capacidad de almacenamiento de esta, y finalmente las innovaciones del hardware físico (los ordenadores como procesadores de datos). Los actores sociales que intervienen en este tipo de sociedades según Castells son los usuarios (ciudadanos, empresas, administración pública y gobiernos), los actores técnicos (la propia infraestructura técnica: los terminales, las redes y los servidores donde se almacena toda esta información), y finalmente los contenidos (que pueden ser tangibles o intangibles, servicios o infomediación). La sociedad de la información afectaría a todos los campos de la socialización y la vida en comunidad: la economía, la legislación, la formación, la cultura, la promoción y las actitudes en general (Castells, 2003). Lo que caracteriza la revolución tecnológica actual no se sólo el carácter central del conocimiento y la información, sino "*la aplicación de este conocimiento e información a aparatos de generación de conocimiento y procesamiento de información/comunicación, en un círculo de retroalimentación entre innovación y sus usos" (*Castells, 1999: 43).

Desde sus inicios hasta los años 90's, Internet vivió una época libre de capitalismo, dada su ausencia de monetización, y hasta cierto punto libre de la intervención

gubernamental. La creciente monetización de la red empieza cuando esta se convierte en lugar de comercio, inicialmente de bienes no físicamente disponibles, momento en que desde los gobiernos de los diferentes Estados y algunas corporaciones internacionales empieza a percibir la necesidad de que el comercio a través de Internet fuera más seguro, facilitando todavía más el desarrollo de monetización de la red. Además del aumento de la velocidad de la conexión y la capacidad de almacenamiento, dos factores han contribuido a este proceso de monetización: la bajada de precios y el aumento de la accesibilidad. Siguiendo al experto en seguridad informática Bruce Schneier, en cualquier sociedad, un desarrollo exponencial de la tecnología hace que se multipliquen los mecanismos del poder *en general*. En el caso de Internet, en un inicio fue un tipo de poder *distribuido* el que ganó territorio: la carencia de una regulación y legislación de la red permitió la emergencia de este poder descentralizado, puesto que esta nueva herramienta proporcionó coordinación y eficiencia a las masas y al ciberactivismo. Hablamos de poderes tanto en sentido positivo como en negativo: movimientos sociales de base, grupos de disidentes, *hackers,* delincuentes cibernéticos, etc. Esto fue posible puesto que las restricciones que instaura el poder tradicional todavía no se adaptaron a este nuevo contexto (Schneier, 2012) El poder distribuido en la red en sus inicios parecía invencible; su potencial se expresó por ejemplo en la llamada "primavera árabe" y la caída entre otros del dictador Mubarak en Egipto en gran parte gracias a las redes sociales. Pero poco a poco, los poderes *tradicionales* han encontrado y establecido nuevas de formas de control sobre lo que sucede en la red: se trata de poderes institucionales organizados, como por ejemplo los gobiernos o algunas grandes corporaciones internacionales.

Según Schneier, este progresivo avance de los poderes tradicionales, además de la ya mencionada monetización de la red, se debe al nacimiento y expansión de la *vida nube* de los individuos: el conjunto de manifestaciones de estas a red, que se encuentran alojados en servidores de corporaciones privadas como por ejemplo Google, Apple, Microsoft o Facebook. En este sentido, las limitaciones que impone el poder tradicional pueden ser de dos tipos: aquellas que afectan directamente a las libertades de comunicación y movimiento (como puede ser el caso de la censura), y por otro lado, lo que nos ocupa aquí: las interferencias en el derecho a la privacidad de los ciudadanos.

El Big Data

El Big Data (a partir de ahora BD) es un fenómeno diferente de propio Internet, a pesar de que este último ha permitido su eclosión, dado que ha hecho mucho más fácil, rápido y barato recopilar y compartir datos. Si Internet ha revolucionado completamente la manera en que se comunica la humanidad, el BD ha supuesto una nueva manera de procesar la información a nivel global. El BD suele ser un concepto pobremente definido: se puede entender simplemente como el cúmulo de datos

suficientemente grande como para tener que ser analizado con grandes computadoras, pero actualmente vemos como también puede ser analizado con ordenadores de sobremesa con un software estándar. Cuando nos referimos al BD, tendríamos que tener en cuenta, no tanto a la medida del agregado de datos, sino más bien a la capacidad de buscar, agregar y cruzar diferentes conjuntos masivos de datos (Boyd & Crawford, 2012), de manera que el potencial del BD se multiplica mediante el uso de tecnologías cruzadas (Cumbley & Church, 2013). Esta explosión en la producción y almacenamiento de datos es relativamente nueva. Si seguimos a Montuschi, en 2000, sólo una cuarta parte de la información almacenada a nivel mundial era digital. El resto se conservó en papel y otros medios analógicos. Pero dado que la cantidad de datos en formato digital se expande tan rápidamente (se multiplica aproximadamente por dos cada tres años), esta tendencia se ha visto invertida: hoy en día, menos del 2% de la información almacenada no es digital (Montuschi, 2005).

Si hablamos de datos, información o conocimiento, hay que tener presente las diferencias entre estos conceptos. El BD empieza a menudo con la creación de datos no estructurados (*raw data),* que no serían sinónimo automático de información. Tampoco la información no puede ser considerada directamente como conocimiento. Previamente tendría que ser clasificada, o si se prefiere estructurada (es decir, procesada de alguna manera). De este procesamiento es de donde tendría que surgir lo que entendemos por conocimiento. Los datos pueden existir en bruto, de una manera que no es necesariamente utilizable, y por lo tanto no tendrían un significado autónomo (por sí mismos): los *datos* deben ser ubicados en un contexto concreto para convertirse en *información,* y si desaparece el contexto, también así lo hará la información. En resumen, el acceso a cantidades cada vez más grandes de información no tiene porque tener necesariamente como resultado un aumento del conocimiento (Schönberger, 2013). Por lo tanto, para entender el BD, hay que resaltar también el papel de los expertos, tanto de las tecnologías (que determinarán la naturaleza de la recolección de estos datos), como de los procedimientos para su explotación (los técnicos en BD).

El uso de grandes volúmenes de información que requiere el BD produce necesariamente tres cambios profundos en la manera nos que percibimos los datos. La primera consiste en recopilar y utilizar una gran cantidad de datos, en vez de pequeñas cantidades o muestras, como se ha hecho desde la ciencia estadística durante siglos. La segunda es que los beneficios del uso de muchísimos datos con una calidad variable pueden resultar mayores que los que nos aportan menores cantidades de datos que sean más exactos. En tercer lugar, en muchos casos, abandonar la investigación de la causa de los fenómenos a cambio de aceptar las correlaciones. Así, estamos recogiendo y analizando cantidades masivas de información sobre los acontecimientos y todo el que se asocia a ellos, buscando patrones que ayuden a la predicción de estos en un futuro (Schönberger, 2013).

Así lo anticipó Alvin Toffler en "La Tercera Ola", refiriéndose al nacimiento del que

este autor bautizará como "la infoesfera": *"Cuando surge un problema tratamos inmediatamente de descubrir sus causas (...) cuando nos acercamos a un problema verdaderamente complicado (...) tendemos a centrarnos en dos o tres factores y a pasar miedo alto muchos otros que, individual o colectivamente, pueden ser harto más importantes. (...). Debido a que puede recordar e interrelacionar gran número de fuerzas causales, el computador puede ayudarnos a abordar talas problemas a un nivel más profundo de lo habitual. Puede cribar grandes masas de datos para encontrar sutiles pautas, reunir "destellos" y congregarlos en unidades más amplias y significativas. (...) Puede incluso sugerir imaginativas solucionas a ciertos problemas mediante la identificación de relacionas nuevas, o hasta entonces inadvertidas entre personas y recursos"* (Toffler, 1980: 179)

En resumen tenemos que entender el concepto de Big Data como la interacción entre tres puntos. En primer lugar, una nueva tecnología, que tiende a la maximización del poder de computación y a la vez perfección de los algoritmos para recoger, analizar, linkar y comparar grandes cantidades de datos. En segundo lugar, un nuevo tipo de análisis derivado de esta tecnología, que consiste en la identificación en estos agregados de datos de patrones y tendencias de las demandas económicas, sociales, técnicas y legales. Finalmente, nos encontramos ante una nueva mitología: la creencia generalizada de que el BD ofrece una forma superior de inteligencia y conocimiento que puede generar percepciones previamente imposibles (Boyd & Crawford, 2012). La explotación del BD puede tener dos vertientes: aquella que se ocupa de la población en general y aquella que se fija en la identificación de conductas que se pueden asociar a individuos concretos de esta población.

En el primer caso, un ejemplo claro seria Google Flue Trends, el estudio de llevado a cabo por Google, que facilita inferir la incidencia real de la enfermedad de la gripe de manera global a partir del análisis de las búsquedas realizadas por los usuarios. La plataforma de servicios de la sociedad de la información (PSSI) Google es hoy una de las principales proveedoras de servicios y plataformas de difusión de contenidos a Internet, gran parte de ellos gratuitos[1]. Además, en muchos casos se requiere la identificación del usuario para utilizar los servicios, asegurándose así el acceso a una cantidad ingente de información cruzada y al mismo tiempo multinivel. Esto ha hecho que hoy en día Google sea probablemente el máximo poseedor de información y datos personales sobre los usuarios de Internet, y por lo tanto se trata de un actor clave en el fenómeno del BD.

En la segunda vertiente, el BD nos permite ver (e inferir) pautas de comportamiento individuales mediante varias conexiones entre variables que contiene esta nube de datos (Montuschi, 2005). Un ejemplo de este segundo uso lo encontramos en el caso de las empresas que utilizan estas técnicas para detectar sectores de la población o

[1] En primer lugar, se trata de un buscador de información en la red y un servidor de correo electrónico (Gmail). También se un navegador web (Chrome), un calendario (Calendar) y un sistema operativo móvil (Android). Se también un sistema de navegación GPS (Navigator), así como un mapa (Maps) y un visualizador de entornos urbanos (Street View) y de la Tierra (Earth). Por el que hace plataformas online, posee Youtube (videos), Blogger (blogs), Picassa (imágenes), y GoogleDrive (almacenamiento de archivos en la nube).

mercados más propensos a consumir sus productos, incluyendo también el diseño de publicidad personalizada *(targeted advertising).*

De esta manera, podemos ver el BD desde dos perspectivas. Desde la perspectiva positiva, la investigación con cantidades masivas de datos puede ser una herramienta de análisis y creación de conocimiento, para unos mejores servicios y bienes públicos (Montushi, 2005). También nos puede puede aportar comprensión sobre los movimientos políticos, así como comunitarios (tanto online como fuera de la red). Desde la perspectiva negativa, puede suponer desde la simple invasión de marketing personalizado, la vulneración de los derechos de privacidad, la reducción de las libertades civiles (como por ejemplo la protesta o la libertad de expresión), así como el aumento del control estatal y corporativo sobre los individuos. Finalmente, varios autores verán como, con la cada vez más automatizada recogida de información y procesamiento de esta, se hace necesario saber cuáles son los sistemas que están guiando estas prácticas, así como la creación de un marco legal que se adapte al contexto cada vez más rápidamente cambiante.

La privacidad

Si seguimos a Arthur Schafer en "Privacy: a philosophical overview" existe cierta confusión, tanto dentro de cómo fuera de la ley, respecto a la naturaleza del interés que el derecho a la privacidad tiene que proteger (Shafer, 1980). La definición de la privacidad que puede resultar en un principio más intuitiva se la de "el derecho a no ser interferido" (*being let alone*), es decir, a permitir que el individuo viva con el mínimo de interferencias posibles. Cuando hablamos de una invasión de la privacidad, generalmente solemos referirnos a algún tipo de interferencia coercitiva al individuo. Es lo que desde la filosofía se denomina *libertad negativa*. Pero, esta definición tiene algunos problemas: el derecho a la privacidad entendido como libertad negativa puede consistir en una definición demasiado ancha o demasiado estrecha. Demasiado ancha, puesto que puede existir coerción sin pérdida de privacidad, y demasiado estrecha, puesto que se puede violar el derecho a la privacidad de una persona sin coerción o interferencia en su vida. La ausencia de una afectación psicológica de la persona no excluye la violación de la privacidad en si, puesto que este mal puede darse o no. En otras palabras, las leyes que protegen el derecho a la privacidad pretenden evitar que los individuos sufran, pero vemos que una definición que haga equivalente la privacidad con la ausencia de mal no incluiría las situaciones en que puede existir una violación de la privacidad sin ningún cambio psicológico en la persona. Además de esto, nos encontramos con que el derecho a la privacidad y el derecho en la no interferencia a menudo se encuentran en conflicto: por ejemplo, para proteger la privacidad de alguien puede ser necesario interferir o limitar la libertad del resto para espiarlo o publicar información sobre él (Shafer, 1980). Otros autores apuntarán a que la mera disponibilidad de información personal no equivale a la invasión de la privacidad: hace falta que esta sea utilizada

con motivos injustificados o claramente malévolos. También sabemos que se puede dar una pérdida de privacidad sin que los individuos vean violado su derecho a la privacidad: tal sería el caso de una filtración de datos personales, fenómeno también propiciado y magnificado por el nacimiento de Internet y el Big Data.

Según Alan Westin, uno de los primeros autores en conceptualizar el derecho a la privacidad, este consiste en "*la voluntad de los individuos, grupos o instituciones de determinar por ellos mismos cuando, como y para que la información sobre ellos mismos es comunicada con los otros*" (Shafer, 1980). En otras palabras, una autorregulación de la imagen que ofrecemos al resto. Esto significa concebir de manera disposicional la privacidad: esta tiene que ser entendida como por un lado, la no interferencia en los asuntos privados de un mismo, y por otro, el control sobre la comunicación de la información de un mismo (y sobre quién puede sensiblemente tener acceso a esta). El ideal de la privacidad es, en general, muy valorado a las sociedades occidentales. Para preservar el sistema democrático, por ejemplo, los individuos tienen que ser capaces de comunicarse y expresarse sin la vigilancia de los gobiernos (Shafer, 1980).

Según García Añón, S. Mill fue quién propuso las bases de algunos de los argumentos que justifican la importancia psicológica, sociológica y política de la privacidad individual: la correlación entre la disponibilidad de un espacio protegido de privacidad y la capacidad del individuo libre para desarrollar su individualidad y creatividad (Añón, 1993).

La privacidad en la Era Digital

La Declaración Universal de las Naciones Unidas de 1948 en su doceavo artículo afirma que "*nadie será objeto de injerencias arbitrarías a su vida privada, su familia, su domicilio o su correspondencia. Toda persona tiene derecho a protección legal ante tales injerencias*".

Pero, en las sociedades modernas, la privacidad se ve sometida a un proceso de erosión. Los factores que producen esta erosión son dos: en primer lugar, la necesidad del mercado de disponer de "*información sobre los actores sociales que participan en él para el funcionamiento de la economía de mercado"*. En segundo lugar, el individuo "*necesita poner en circulación su información para realizar intercambios y negocios de diferentes tipos*" (Sánchez, 2003: 39). Por otro lado, para el buen funcionamiento de las sociedades plurales desde el punto de vista ideológico, también sería deseable que quede garantizado el acceso público determinada información (es decir, el equilibrio entre el *derecho a la privacidad* y el *derecho a la información*). El Estado también tiene que disponer de información sobre sus ciudadanos para poder implementar políticas de todo tipos, incluidas las medidas de seguridad (es decir, el equilibrio entre *el derecho a la privacidad* y la seguridad). Hablaremos de estos dos equilibrios más adelante**.**

Para Ana Victoria Sánchez, en este contexto, el derecho a la privacidad aparecerá, ya no como el derecho a decidir qué tipo de información se comparte, sino como *"el derecho a controlar el uso que las instituciones públicas o privadas hacen de la información de los ciudadanos*" (Sánchez, 2003: 42). Según esta autora, las nuevas tecnologías de la información y comunicación permiten dos nuevos tipos de vulneraciones del derecho a la privacidad: por un lado, la difusión masiva a través de Internet, y por el otro, el uso de bases de datos ilegítimas. Las leyes y regulaciones para la protección de la privacidad en la red hacen referencia a la organización y requerimientos técnicos con los que se pretende proteger los datos personales que son almacenados y procesados por los sistemas informáticos. Esto incluye desde la obtención lícita de los datos, la notificación al usuario de los propósitos por los que se utilizarán, y también los sistemas mediante los cuales el usuario debería poder supervisar el procesamiento de la información que se recoge sobre él. Desde el campo del derecho, el tipo de contenido y la voluntad del emisor de la información determinarán tres tipos de "esferas" de privacidad de la información, ya sea en la red o fuera de esta. En primer lugar, tendríamos la información *estrictamente privada*. Esta incluiría aquella información que el individuo emisor tiene la voluntad de que sea privada, cuyo destinatario sería único: seria determinada (no indeterminada), puesto que excluiría a cualquiera otro destinatario. En esta categoría se incluirían los mensajes y correos electrónicos, así como contenido analógico y digital diverso que cumpla las características anteriores. En segundo lugar, tendríamos la información semiprivada o *semipública*, que sería toda aquella que el emisor decide mostrar a un destinatario(s) o sujeto(s) de su elección. Por lo tanto, no sería individualizada, de forma que los destinatarios no tendrían derecho a hacerla pública o difundirla en una esfera que no sea la que el emisor ha escogido. Es decir, los receptores no tendrían facultad de *disposición* de esta información. Un ejemplo sería el contenido publicado en redes sociales como Facebook (dependiendo de la configuración de privacidad que escoja el usuario). En tercer lugar, tendríamos la información pública, que incluiría cualquier publicación que no tenga restricción de acceso. Esta información sería *voluble*, en el sentido de que puede ser transmitida, reproducida y recopilada por el público en general, siempre que se haga de una manera fidedigna (sin tergiversarla o manipularla). Esta categoría incluiría la gran mayoría de la información disponible en Internet (lugares web, blogs...etc).

Nuevos retos para la privacidad

Este apartado se centra en dos tipos de retos a los que se enfrenta la privacidad: en primer lugar, lo que desde la sociología puede llamarse nuevo paradigma de las relaciones interpersonales en Internet, y en segundo lugar, la colisión del derecho a la privacidad con dos derechos más: *la seguridad* y el *derecho a la información*. En general, el reto más importante al que se ve sometido el derecho a la privacidad de los usuarios de Internet es la recolección de datos a gran escala por parte de gobiernos y corporaciones, incluyendo, entre otros, las comunicaciones electrónicas,

el rastreo de las acciones a la red (gracias a las cookies, términos de búsqueda web...etc), información sobre localización vía GPS (gracias a los dispositivos móviles u otros conectados a la red o los sistemas de vídeo-vigilancia), o la información financiera. Así, el tipo de información personal que se puede obtener es de lo más variopinta: datos sociodemográficos, comunicaciones (emails y mensajería), archivos en la nube, ubicación física, gustos y preferencias, información financiera, patrones de consumo o historial médico entre otros. Todos estos cambios son irreversibles, y la consecuencia directa de vivir en un mundo cada vez más electrónico y digitalizado (Cumbley & Church, 2013).

Si hablamos desde el campo de la sociología, se está produciendo, sobretodo en las sociedades avanzadas, un nuevo paradigma de las relaciones y vínculos interpersonales. A medida que más y más gente utiliza las redes sociales online, estas han acabado sustituyendo una parte de las propias relaciones cara a cara, convirtiéndose en una importante herramienta con la que las personas se comunican y expresan. Respecto a los motivos psicológicos por los cuales la gente comparte información personal, nos dicen que el uso de las redes sociales como Facebook se da por el deseo de conocer y aprender del resto de individuos (Joinson, 2008), y que por lo tanto, tal cosa no sucedería sin compartir información personal en la plataforma. Además, cabe no olvidar que también las comunicaciones *privadas* entre individuos cada vez son más digitales, aumentándose los riesgos de exposición a la vulneración de su privacidad.

Equilibrio entre el derecho a la privacidad y la seguridad

En el caso del equilibrio entre el derecho a la privacidad y la seguridad, según el Joint Research Center de la Comisión Europea existen dos factores que afectan actualmente a este difícil equilibrio: por un lado, la implantación de las nuevas tecnologías de la información, y por el otro, las reacciones de los gobiernos al aumento de la delincuencia y el terrorismo. Así, se habla de un cambio en el *modo de protección* de la seguridad: se ha pasado de una seguridad *activa* a una seguridad *reactiva*, cosa que ha derivado en un "*aumento de la capacidad de los gobiernos de acceder a información de los ciudadanos que sobrepasan los motivos por los cuales esta ha sido suministrada inicialmente".* Actualmente, vemos como la tendencia desde los Estados es atender a las demandas de aumento del control sobre las actividades de los ciudadanos en la red, como vemos en el caso de la reforma del código penal en España, con el objetivo de mejorar la lucha tanto de los delitos como de los ciberdelitos.

Un ejemplo de ello sería el programa PRISM del gobierno de Estados Unidos, que involucra a la NSA (la Agencia de Seguridad Nacional Norteamericana) en la recolección y análisis de los datos y comunicaciones personales, también de otros países, de diferentes fuentes, incluidas las corporaciones Apple, Facebook, Microsoft, Google, Yahoo, YouTube, Skype, AOL y PalTalk. Un informe completo del

funcionamiento de este programa de espionaje a gran escala fue desvelado por el ex-trabajador de la NSA Edward Snowden. Las empresas implicadas en un inicio negaron su colaboración, pero poco a poco las evidencias muestran que la mayoría de ellas eran conocedoras de las actividades que desarrollaba la NSA. En Estados Unidos, la ley *Foreign Intelligence Surveillance Act* (FISA) determina que el gobierno tiene el derecho a solicitar datos referentes a los usuarios a los operadores y proveedores de servicios de Internet, pero sólo después de que así lo determine un juez. Según el informe que publicará un tiempo después la propia NSA[2], vemos como esta invasión de la privacidad queda justificada por la intención de prevenir tanto futuros ataques terroristas como el cibercrimen, sobretodo después de los atentados del 11 de Septiembre.

Equilibrio entre el derecho a la privacidad y derecho a la información

El control de la información personal, contendría dos aspectos: por un lado, la posibilidad de mantener ocultos algunos de los aspectos de nuestra vida, y por el otro, la opción de poder controlar el tratamiento y transmisión o circulación de la nuestra información un vez se exponga a un tercero. El derecho a la información incluiría la capacidad positiva de transmitir y hacer conocer la información, y por otro lado, el derecho a ser informados, así como a investigar para obtener o acceder a esta información. Podemos decir que el derecho a la privacidad y el derecho a la información colisionan, en el sentido que existe un conflicto entre ambos, puesto que el ejercicio de uno excluye de alguna manera el otro.

Ante esta colisión existirían cuatro posiciones: ver que el derecho a la privacidad está por encima del derecho a la información, ver que el derecho a la información está por encima del derecho a la privacidad, una posición mixta (donde ambos derechos serían equivalentes) y finalmente una cuarta posición, en la que tendría que ser valorado según las circunstancias en el momento que la colisión de estos derechos se produzca (Muñoz Peralta, 2008). En la primera posición, la idea subyacente es la de la privacidad ese derecho ser dejado vivir en paz, asumiéndose la necesidad de un espacio reservado para la creación de la persona independiente del resto de agentes sociales. La segunda posición, otorgará preponderancia al derecho a la información, dado que se considera que si se viola el derecho a la libertad de expresión, se está vulnerando un derecho que acaba siendo el que garantiza el resto de derechos. La posición mixta, verá como, dependiendo de si se trata de información de interés general o no, un derecho prevalecerá sobre el otro. Por último, la posición jurisdiccional, como por ejemplo la que adopta la Constitución Española en su artículo 18 cuando hace referencia a que *"la limitación del uso de la informática tenderá a respetar no sólo el honor y la intimidad de la persona, sino el ejercicio del todos los derechos"*.

[2]Documento Dficial de la NSA (2013) https://www.documentcloud.org/documents/750221-2013-08-09-the-nsa-story.html

Recientemente, Google ha creado un formulario online para ejercer lo que algunos han llamado "derecho al olvido en la red" después de una sentencia del Tribunal de Justicia de la Unión Europea. La sentencia viene motivada por el caso de un hombre español que denunció que Google enlazaba a un periódico online donde se podía encontrar información referente a unas deudas que había tenido con la seguridad social. Sostenía que Google y el diario tenían que eliminar esta información, puesto que violaba su derecho a la privacidad, además de no ser un reflejo de su situación actual. El Tribunal de Justicia dictaminó que el diario podía dejar la información publicada en su sitio web, pero que Google tenía que eliminar los enlaces a esta en sus resultados de búsqueda. Google fue instado a borrar esta información puesto que es una empresa que recopila gran cantidad de datos y las procesa, entre otras, se incluye información sobre las personas, y según la Directiva de Protección de Datos de la UE, los responsables del tratamiento de datos personales tienen obligaciones especiales, incluyendo la responsabilidad de eliminar los datos que son *"insuficientes, irrelevantes o ya no relevantes"*. Esto no significa que la empresa tenga que borrar automáticamente la información de sus resultados de búsqueda, sino que el interesado lo tiene que solicitar y Google después tendrá que sopesar si considera que la información debe mantenerse enlazada. Si nos fijamos, vemos como esta decisión va en contra de la libertad de información (y expresión), además de dar todavía más poder a Google, dado que hace responsable a esta corporación de filtrar y determinar en qué casos se trata de información de interés público, de alguna manera convirtiéndolo en juez, y en realidad no se esta resolviendo problema subyacente, que continúa encontrándose en el contenido en si, y no el enlace que dirige hacia este. Además, algunos autores apuntan a la inviabilidad de la supervisión por parte de los PSSI de la ingente cantidad de información que manejan (Sánchez, 2003).

La mercantilización de la información personal

Los datos personales se han convertido ya en un bien básico, mediante el cual se crean otros bienes, "*convirtiéndose en una mercancía más en el proceso de producción, intercambio y consumo"* (Sánchez, 2005). Tal y cómo apunta el informe del World Economic Forum "Rewards and Risks of Big Data" (Bilbao-Osorio et al. 2014), los datos son hoy en día un nuevo tipo de mercancía que puede ser comparado con el oro o el petróleo en revoluciones económicas anteriores. Pero, así como el petróleo es una materia prima escasa, los datos nunca serán escasos, puesto que son continuamente producidos por nuestro estilo de vida moderno, en combinación con las tecnologías de la información y comunicación. Este informe se muestra preocupado por los nuevos tipos de infracciones al derecho a la privacidad que no se encuentran regulados por la actual legislación. Las recomendaciones del World Economic Forum en este campo estarían enfocadas principalmente en aumentar la confianza en las aplicaciones del Big Data para sacarle todo su potencial: la definición de lo que se debe considerar como información personal, como tratarla,

en qué casos se puede aplicar el "derecho al olvido" y por último, la necesidad de clarificar la jurisdicción relevante en este campo. Las políticas que desde este organismo se recomiendan serían entre otras la separación de las bases de datos por tipos (por ejemplo, financieras-salud) y según si son referidas en el mundo real (individuales-corporativas). Con estas precauciones, se haría más complicado atacar diferentes tipos de datos a la vez, y también se dificultaría la combinación de los tipos de datos sin una autenticación previa de los sistemas de gestión de estas bases diferenciadas. Se recomienda por ejemplo, el etiquetado de los datos almacenados con un código de software que indique las preferencias de privacidad que han escogido los usuarios de manera predeterminada.

Corporaciones como Google o Facebook han creado productos y plataformas que constituyen mercados propios, ofreciendo sus servicios de manera gratuita, y la participación de los individuos comporta necesariamente la aceptación de las condiciones que estas ofrecen. En el caso de Facebook y otras redes sociales (como por ejemplo Myspace), es de dominio público que han hecho negocio enviando información a los anunciantes que se podría utilizar para encontrar los nombres de los consumidores y otros detalles personales. Se podría decir que todo el *raw data* que generan los usuarios es una mercancía inerte, esperando a ser modelada y procesada para producir los materiales que necesitan las industrias que se dedican a sacar provecho de toda esta agregación de datos. Dado que el usuario no tiene ningún control sobre los mecanismos que luego darán forma a estos datos, estos se acaban convirtiendo en algo con usos potenciales ilimitados. Los datos como mercancía tienen una otra característica: a diferencia de las materias primas físicas, que se agotan o resultan más caras de producir, los datos no se pueden agotar, y una vez que han sido vendidas no desaparecen. Por otro lado, si definimos la plusvalía como el aprovechamiento del trabajo excedente de los trabajadores por parte de los propietarios de los medios de producción sin una compensación a cambio, *"la vigilancia y monitorización de las transacciones e interacciones de los individuos juega un papel muy importante en este proceso, dado que producen un exceso de información",* el valor de la cual vendrá dado por su utilidad para la creación de perfiles de consumidores y estudios sobre nuevos sectores del mercado (Andrejevic, 2007).

Recientemente, la Federal Trade Comission de los Estados Unidos ha publicado un informe donde se explican las prácticas de los "data brokers", que trabajan en empresas dedicadas a la explotación del BD. Los data brokers recolectan información de numerosas fuentes, en muchos casos sin el consentimiento de los usuarios, y también comparten información entre ellos. Estas fuentes pueden ser comerciales, gubernamentales y otras fuentes de información públicas. A pesar de que las fuentes a menudo sólo aportan algún aspecto de la actividad de los consumidores, su agregación puede tener como resultado una visión más completa de los hábitos de los usuarios y consumidores. Así, se dedican a utilizar la combinación de elementos para crear listas de consumidores que tienen características similares, desarrollando

modelos complejos para la predicción del comportamiento de estos. El informe apunta al peligro que estas prácticas suponen, centrándose sobretodo en que pueden resultar una herramienta en pro de la discriminación de los individuos. A pesar de que no se trata de Europa, esta preocupación también se ha hecho patente, puesto que recientemente se ha llevado a cabo una reforma del reglamento Europeo de Protección de Datos, que contempla que los usuarios se opongan a la creación de perfiles de consumidores con sus datos personales, y por otro lado lo prohíbe cuando se tenga como objeto el discriminar a las personas.

Por otro lado, estamos viendo como el sector del marketing digital tiende a segmentar y individualizar la publicidad por la que se paga online; de hecho, estamos asistiendo a su conversión a sistema de puja de los anunciantes para aparecer en un momento y ocasión determinados al usuario (ver AdSense de Google), para asegurarse así obtener el máximo potencial a su inversión en publicidad y fidelizar a sus consumidores. Esto hace que también se haga previsible un incremento de las tecnologías para la recolección de datos sobre los usuarios.

Actitudes de los ciudadanos ante sus datos personales

Desde el ámbito de la sociología y la economía, el papel de los usuarios es clave desde dos puntos de vista. Por un lado, la actitud que estos adoptan ante la divulgación o uso de sus datos, y desde el otro, desde el punto de vista de los intereses de la monetización de la red, con el objetivo de estudiar la confianza que los usuarios tienen con las diferentes herramientas digitales de consumo. Según el Eurobarómetro de la Unión Europea del 2011, la mayoría de los ciudadanos europeos considera la divulgación de su información personal como una parte intrínseca de la vida moderna. Este estudio distingue entre dos tipos de usuarios, que mostrarán actitudes diferenciadas por lo que respecta la divulgación de su información personal: por un lado, los usuarios de las redes y plataformas sociales, y por el otro, los compradores online. Mientras que más de la mitad se oponen a la creación de perfiles con sus datos, los riesgos que más perciben los usuarios en general son tres: por un lado, ser víctimas de fraude (sobre todo en el caso de los compradores online), por otro lado, el uso de sus datos sin su consentimiento, y finalmente, el uso de estas por parte de terceros.

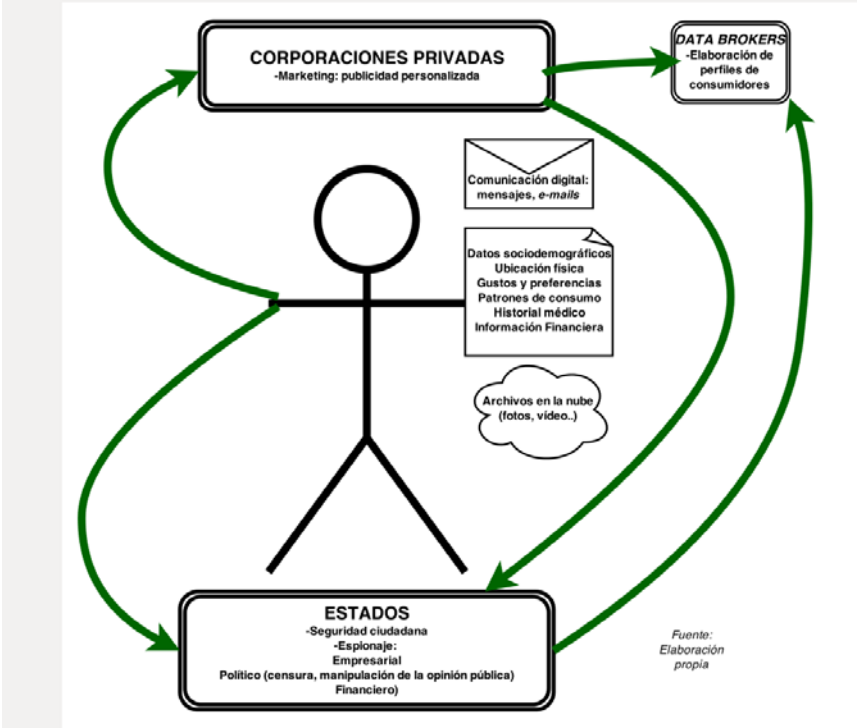
En el intento de protección de sus datos, los europeos utilizan más estrategias *pasiva*s (sin acción propiamente dicha), es decir, limitar la información que publican o la reducción de su huella digital.

Un 60% dice leer las políticas de privacidad de las plataformas y lugares online que visitan, mientras que un 30% dice no ser informado debidamente de estas. Un 25% (cifra aún menor en el caso de los compradores) dice sentir un control total sobre sus datos en la red. Sólo un tercio de los europeos conoce la existencia de un organismo nacional de protección de datos en sus respectivos países, y casi la mitad dicen confiar más en las instituciones supranacionales europeas para este fin.

Si nos fijamos en las diferencias entre países, los usuarios del sur de Europa son más propensos a experimentar que su información personal esta siendo utilizada sin su consentimiento.

Existe también una diferencia entre los usuarios *nativos* (aquellos que han nacido y crecido en la era digital) respecto de aquellos iniciados en edades más avances en el uso de las nuevas tecnologías. El primero es menos propenso a considerar que la divulgación de su información sea un problema, y tienden a leer menos las políticas de privacidad. El segundo grupo, en general, tiende a protegerse más, cambiando por ejemplo la configuración de las plataformas que así lo permiten, con el objetivo de proteger su información. En general, el hecho de leer las condiciones de privacidad de las plataformas y sitios web hace cambiar sensiblemente el comportamiento online de los usuarios.

Otro estudio, en este caso en Estados Unidos, y únicamente analizando los comportamientos de usuario de webs comerciales, apunta a la poca adecuación de las políticas y sistemas de protección de datos de la mayoría de webs para la comprensión del usuario (Teltzrow & Kobsa, 2004). Este estudio desvela que mientras la mayoría de usuarios de muestran preocupados por su privacidad, muchos no actúan consecuentemente, es decir, no mantienen una actitud *activa* ante la protección de sus datos. Una gran parte de los usuarios desearía que se le pidiera permiso en caso de que su información fuese utilizada con fines de marketing, más del 75% cree que las políticas de privacidad son muy importantes, y más de la mitad piensa que estas le aportan confianza al proporcionar sus datos. Así, si se pretende hacer aumentar la confianza de los consumidores, son necesarias nuevas herramientas que informen al usuario sobre el impacto o consecuencias de la gestión de su información personal de una manera amigable concreta y en cada momento.



Fuente: Elaboración propia

Conclusiones

Una vez vista la incipiente pero creciente sinergia que actualmente se está produciendo entre los poderes privados y los Estados al utilizar los datos personales que los usuarios generan en la red, las conclusiones que podemos extraer son desde diferentes campos. En general, podemos afirmar que la digitalización de la información nos enfrenta a una serie de retos que acabarán por ser ineludibles en las sociedades modernas capitalistas, y afectarán sin ningún tipo de duda a los equilibrios de poder del futuro. La hipótesis de Schneier es que, dado el aumento del poder derivado de la innovación tecnológica, en un momento de rápidos cambios, este poder es a menudo aprovechado por los actores sociales para actuar en beneficio propio, creándose nuevos dilemas sociales que requieren de una actuación igualmente rápida y eficaz si se quieren garantizar los equilibrios de poder. En un momento en que la tecnología cambia tan rápidamente, los mecanismos de protección de la privacidad de los ciudadanos deberían adaptarse también rápidamente, pero para poder hacerlo a tiempo, las leyes que se formulen en un futuro tendrían que ser válidas tanto por entornos reales como por entornos digitales, puesto que de una otro manera estas tendrían que ser continuamente reformuladas por la irrupción de los nuevos riesgos que la tecnología facilita (Shneier, 2012). En este contexto del salto de la privacidad real a la privacidad digital, los mecanismos para su defensa tienen que ser replanteados, adaptándose a las nuevas circunstancias que estas tecnologías han hecho emerger: Así, como conclusiones técnicas, haríamos referencia a la necesidad de comprender el funcionamiento de los mecanismos que operan en todo este fenómeno. Ya sea para proteger el derecho a la privacidad del usuario, como para aumentar su confianza en la red, se hace necesaria una simplificación de las políticas de privacidad, para facilitar que estos tomen decisiones conscientes e informadas respecto a la divulgación o exposición de su información. Nos encontramos con que, aunque la gran mayoría de usuarios y consumidores utiliza internet en cada vez más aspectos de su vida, muchos tienen un desconocimiento de políticas de privacidad, y también es previsible que este hecho se vea propiciado por la aparición de aparatos tecnológicos cada vez más fáciles de utilizar. La situación actual de carencia de una regulación clara, la defensa de la privacidad debe ser *activa*, con un necesario un aumento de la cultura informática por parte de los usuarios. Aun así, se trataría sólo de medidas provisionales, puesto que se hace complicado abordar esta problemática sólo con soluciones tecnológicas que requieren una toma de medidas *activas* por parte de los usuarios.

Respecto a las conclusiones en el campo de la legislación, dado que se trata de un problema global, y los datos no entienden de fronteras, las leyes para su regulación tendrían que venir dadas desde instituciones supranacionales, y no con el actual modelo legislativo centrado en los Estados.

Como conclusiones sociológicas, dado que las relaciones personales son cada vez más digitalizadas, se hace más urgente la toma de medidas políticas y legales. Las

políticas y leyes que nos tendrían que proteger contra este tipo de explotación de la información personal son todavía inefectivas. También sería necesario que los castigos en caso de infringirlas fueran suficientemente elevados, para evitar que salga a cuenta vulnerarlas. Una vez visto el beneficio económico que pueden aportar nuestros datos personales, entendemos que se necesario un aumento de la transparencia con la que trabajan los data brokers, así como un incremento del control de los consumidores sobre la información de la que estos disponen, regulando también el derecho de los ciudadanos a la supervisión de sus usos. Finalmente, una vez asumida la necesaria concepción *disposicional* de la privacidad, por la cual no existe este derecho sin la protección ante los potenciales poderes del resto a violarlo, entendemos que la lucha por la información personal es finalmente una lucha por la libertad.

Referencias bibliográficas

Bilbao-Osorio, B.; Dutta, S. and Lanvin, B. (2014) (Eds.): *The Global Information Technology Report 2014 Rewards and Risks of Big Data*, Ginebra: World Economic Forum, Insight Report. Accesible en: http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf Fecha de acceso: 10/03/15.

Boyd, D. & Crawford, K. (2012): Critical questions for Big Data *Information, Communication and Society* 15: 662-679.

Castells, M. (1999): *La Era de la Información: Economía, Sociedad y Cultura*: *La sociedad Red*, México: Siglo XXI.

García Añón, J. (1993): *Una aproximacion al concepto de derecho a la intimidad de J. S. Mill,* Valencia: Universitat de Valencia.

Joinson, A. N. (2008): *Looking at, looking up or keeping up with people. Motives and uses of* Facebook. CHI 2008, April 5–10, 2008, Florencia, Italia. Accesible en: http://onemvweb.com/sources/sources/looking_at_motives_facebook.pdf Fecha de acceso: 10/03/15

Mayer Schönberger, V. y Cukier, K. (2013): *Big data: la revolución de los datos masivos*, Madrid: Turner.

Montuschi, L. (2005): *Cuestiones éticas problemáticas en la era de la información, internet y la world wide web,* CEMA Working Papers, Universidad del CEMA. Accesible en: http://www.ucema.edu.ar/publicaciones/download/documentos/306.pdf Fecha de acceso: 10/03/15.

Muñoz Peralta, H. M.; Carrasco Tapia, J. M.; Mendo Coronel, C. E.; Arcángel Salcedo, E. E. y Romero Mendoza, J. (2008): Conflicto jurídico entre el Derecho a la intimidad y la Libertad de información, *Revista Jurídica Cajamarca*. Accesible en: http://www.ceif.galeon.com/REVISTA3/intimidad.htm Fecha de acceso: 10/03/15.

Toffler, A. (1993): *La tercera ola*, Bogotá: Plaza y Janés.

Sánchez, A. V. (2003) *Tecnología, intimidad y sociedad democràtica*, Barcelona: Icaria.

Schneier, B. (2012): *Liars and Outliers: Enabling the Trust that Society Needs to Thrive and Carry On*, Indianapolis: John Wiley & Sons.

Shafer, A. (1980): *Privacy: A Philosophical Overview*, A*spects of Privacy Law*, ed. D. Gibson, Butterworth, 1980 University of Manitoba. Accesible en: http://umanitoba.ca/faculties/arts/departments/philosophy/ethics/media/privacy_-_a_philosophical_overview.pdf Fecha de acceso: 10/03/15.

Stutzman, F.; Gross, R.; Acquisti, A. (2012) *Silent listeners: the evolution of privacy and disclosure on Facebook* Journal of Privacy and Condentiality (2012) 4/2: 7-41.

Teltrzrow, Maximilian; Kobsa, Alfred, (2004): *A multiple wiew of infidivudal privacy in a networked world,* Wholes, Stockhold, Sweden. Accesible en: http://www.ics.uci.edu/~kobsa/papers/2004-WHOLES-kobsa.pdf Fecha de acceso: 10/03/15

Webgrafía

Artículo 18 Constitución Española. Accesible en: http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2 Fecha de acceso: 10/03/15.

Institute for Prospective Technological Studies (2003): *Seguridad y privacidad para el ciudadano en la era digital posterior al 11S: una visión prospectiva*, Institute for Prospective Technological Studies. Accesible en: http://ftp.jrc.es/EURdoc/20823-ExeSummES.pdf Fecha de acceso: 10/03/15.

Documento Oficial de la NSA 2013. Accesible en https://www.documentcloud.org/documents/750221-2013-08-09-the-nsa-story.html Fecha de acceso: 10/03/15.

Data Brokers: A call for transparency and accountability Federal Trade Comission (2014). Accesible en: http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf Fecha de acceso: 10/03/15.

Eurobarometro Especial 359 (2008): *Attitudes on Data Protection and Electronic Identity in the European Union.* Accesible en: https://open-data.europa.eu/es/data/dataset/S864_74_3_EBS359 Fecha de acceso: 10/03/15