Privacidad y control de datos: evitar que atrapen nuestros datos personales

L. Fernando Ramos Simón[1]
Universidad Complutense de Madrid, España

Introducción

El documento que nos presenta la IFLA[2] explora cinco tendencias que, sin duda, constituyen una buena agenda para analizar la revolución de la información en la que estamos "atrapados", tanto en nuestra condición de ciudadanos como en la de expertos en información. La primera cuestión a determinar es si todas estas tendencias

1 Agradezco al doctor Jaime Ríos la invitación y la oportunidad de participar en este evento y expresar algunas reflexiones. Fue él quien atrajo mi curiosidad sobre este documento al facilitarme el borrador final en proceso de revisión durante una visita que realicé en el otoño de 2013 al IIBI, con motivo de la participación en un proyecto PAPIIT dirigido por el profesor Egbert Sánchez y el encuentro de la Cátedra Gaos promovido por la UNAM y la UCM al que acudí por cortesía de mi Departamento de Biblioteconomía y Documentación.

2 IFLA Trend Report (2013), *¿Surcando las olas o atrapados por la marea? Navegando el entorno en evolución de la información*.

Este artículo forma parte del proyecto "Organización del acceso y uso de la información del sector público. Hacia la consolidación de una industria de la información", dirigido por el autor y financiado por el Plan Nacional de I+D en España (Ref. CSO2010-17451).

arrastran vientos de preocupación o transportan gérmenes de esperanza en la mejora de la educación, la igualdad y la libertad. Repasemos estas cinco directrices:

1. Las nuevas tecnologías de la información expanden a la vez que limitan el acceso.
2. La educación en línea aumenta las oportunidades de aprendizaje, de forma más barata y accesible.
3. La gran revolución en la producción de datos podrá tener graves consecuencias para la privacidad de las personas y su autonomía personal.
4. Una sociedad hiperconectada alumbra la aparición de nuevos grupos y nuevas voces con la promesa de más transparencia y mejores servicios para los ciudadanos.
5. El predominio de las nuevas tecnologías transforma la economía global con nuevos modelos de negocio que se asientan sobre la ubicuidad de esos dispositivos móviles.

Si nos fijamos atentamente, de los cinco aspectos o tendencias, el único que ofrece un enfoque negativo, o lo presenta así en mayor medida, es el asunto de la privacidad y la protección de datos personales, puesto que el acceso fácil y barato a los datos masivos de perfiles personales condiciona y daña la autonomía de los individuos. De alguna forma, la privacidad es el elemento negativo residual de las otras cuatro tendencias, en sí positivas, pues no se pueden calificar de otra forma los grandes avances que prometen las nuevas tecnologías en ámbitos como la educación o en el incremento de la participación democrática.

En un contexto académico, dada la revolución tecnológica en marcha en el ámbito de la información, se ha de

afirmar que el control de los datos personales por cada individuo es ilusorio, debido a la masiva recopilación que de ellos se hace cada día, a su uso como datos secundarios, a la sofisticación de esas herramientas de tratamiento y a la capacidad de transportar esos datos a nivel global a través de sistemas de computación en la nube (*cloud computing*). Además, dada la importancia económica de este comercio *Big data*, los datos personales se han integrado en la economía de la información.

Para comenzar, cabe hacer dos preguntas fundamentales: ¿cuál es el grado de privacidad deseable desde el punto de vista social? ¿Qué consecuencias negativas se derivan para los individuos a causa de la agregación masiva de datos? Por tanto, se abre una tercera pregunta: ¿cómo podemos evitar esos aspectos negativos que se derivan del aluvión de datos masivos generados por los más variados dispositivos de gestión de la información en los más variados entornos (calle, comercio, redes, etcétera), incluso en unidades documentales como las bibliotecas?

La respuesta no puede ser determinista en el sentido de que las consecuencias han de ser negativas *per se*. El hecho de que la tecnología permita fabricar vehículos capaces de alcanzar una velocidad superior a 300 km/h, no implica que cualquier individuo pueda usar el automóvil por cualquier sitio. Al contrario, la conducción a alta velocidad controlada, en circuitos adaptados a ella, ofrece enormes ventajas para la seguridad de todos los usuarios en su vida cotidiana. Veamos estos aspectos, que no admiten una respuesta contundente porque los cambios sociales y tecnológicos obligan a una constante adecuación entre ambas cuestiones.

Sobre la privacidad de los datos: el estatus deseable

Los datos personales son cualquier información que relaciona a una persona con su vida privada, profesional o pública, ya sean imágenes, datos de identidad, cifras bancarias, comentarios en la redes sociales o direcciones IP de los dispositivos utilizados para conectarse a Internet, aunque ni siquiera esta concepción es ampliamente compartida, como señalan Bennett y Parsons (2013, p. 498). En España, el derecho constitucional a la protección de datos "[…] incluye un haz de garantías y facultades que se traducen en determinadas obligaciones de hacer. Se trata del derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelarlos." (Martínez, 2007, p. 50)

La privacidad es un concepto cambiante, muy dependiente de los usos de los grupos sociales y de los momentos históricos; "la vida privada no es una realidad natural que venga dada desde el origen de los tiempos" (Prost, 1993).[3] La historia muestra que hay una correlación entre la vida privada y la vida pública o, como dice más gráficamente Escalante (2012, pp. 15-16), "[…] la separación de lo público y lo privado tal como la conocemos y la institución de un Estado secular son dos caras de una misma moneda."

Tampoco las nuevas tecnologías de la información son la primera amenaza a la privacidad de las personas. No están tan lejos los tiempos en los que, en las sociedades acomo-

3 La visión sobre la evolución de la vida privada presentada en esta excelente obra en cinco tomos sigue siendo válida y queda expresada de una forma contunde en una frase de la presentación de la obra en el tomo 2, al decir de George Duby: "Que el lector no espere encontrar aquí un cuadro acabado. Lo que va a leer, incompleto, repleto de interrogantes, no es más que un esbozo". Suscribimos esas afirmaciones treinta años después.

dadas de cualquier lugar, una boda, por ejemplo, iba precedida de una solicitud de buenos informes al sacerdote o a las "buenas gentes" del lugar de procedencia de los novios. Tampoco es cierto que aquellas sociedades más defensoras de la privacidad se muestran como feroces enemigas de la transparencia. Sirva como máximo ejemplo Suecia, que fue el primer país en legislar para defender la privacidad frente al uso de la informática (1973) y que, a la vez, dispone de la legislación más antigua sobre libertad de información (1766). Así, el hecho de que el país cuente ahora con el Partido Pirata, el primero de estas características con representación en el Parlamento Europeo (el tercer partido del país por número de afiliados), podría ser visto como una señal de que la defensa de la privacidad y de la transparencia no son conceptos antagónicos.

En la Unión Europea, según revelan las encuestas, existe un sentimiento generalizado de que la gestión masiva de los datos es consustancial a la vida actual y, también, que se solicitan más datos personales de los realmente necesarios. Así, un 58% piensa que no hay más alternativa que facilitar esos datos si se quieren obtener productos y servicios. Los datos personales que con mayor frecuencia se facilitan son el nombre, el domicilio y el número de teléfono. En la reforma de la legislación que la Unión Europea puso en marcha en 2012 y que, se prevé, esté concluida en 2020, se propone aplicar dos principios esenciales: privacidad por diseño y privacidad por defecto; de modo que la protección de los datos debe ser un componente esencial en la creación de todos los productos y servicios, a la vez que la protección de los datos sea la norma por defecto. Se pretende al mismo tiempo construir un sistema con una amplia protección de los datos relacionados con la seguridad del Estado y la investigación de actividades delictivas.

Sin embargo, debemos decir que, en el terreno de los buenos propósitos, se choca con el gran potencial que ofrecen las tecnologías de información en el tratamiento de esos datos personales. Así, el concepto de la privacidad por diseño (PET: Privacy Enhancing Technologies), que trata de evitar el uso no autorizado de datos personales y permitir el control a su titular, pese a sus ventajas de facilidad de uso e integración en las herramientas cotidianas, todavía plantea dudas (Bennett y Parsons, 2013, p. 501).

La amenaza de los datos masivos: el Estado, el comercio

Hay una tendencia pesimista en torno al potencial de vigilancia de Internet sobre nuestros datos personales. Amenazas que surgen de las actividades de control que llevan a cabo las compañías mercantiles y los gobiernos.

Por parte del Estado, el principal argumento para utilizar herramientas de datos para el control del espacio público (video-vigilancia, reconocimiento facial, RFID: Radio Frequency Identification, etcétera) o limitar la privacidad de las personas (sistemas de gestión de identidad, monitoreo de redes sociales, etcétera), se asienta hoy en la seguridad pública. Si nos atenemos al estado de opinión en Estados Unidos, el país líder en la promoción de la seguridad, las opiniones aparecen muy divididas.

En una encuesta de mediados de 2013, publicada en el semanario *Time* (24-6-2013), un 48% estaba de acuerdo con las prácticas de control por el gobierno de grabaciones telefónicas, correos electrónicos y búsquedas en Internet; frente a un 44%, que se mostraba en contra. Más clara es la posición de esos ciudadanos sobre si se deberían perseguir

las revelaciones de material clasificado que puede dañar los esfuerzos de seguridad, pues un 53% fue partidario de esa práctica y sólo un 28% opinó que no se debería penalizar "porque el público tiene derecho a saber". Por último, resulta un poco sorprendente que un 43% opinó que el gobierno debería reducir los programas que amenazan la privacidad, frente a un 28% partidario de un equilibrio entre la percusión del terrorismo y la protección de la privacidad, y un 20% partidario de perder privacidad para combatir al terrorismo. Una conclusión clara es que, si los ciudadanos ponderan más la seguridad que la privacidad de las personas, difícilmente los gobernantes van a respaldar actitudes compatibles con el derecho a saber y el respeto a la privacidad de las personas. Si, por el contrario, hay un mayor activismo habrá menos posibilidades de manipulación sobre el conjunto de los ciudadanos, como sugiere nuestro documento interno de reflexión previo al documento final (Síntesis de la discusión de expertos, p. 21).

Se puede decir que la tensión de los gobiernos representativos entre la seguridad y la privacidad como justificación para ejercer un mayor control sobre los ciudadanos y los grupos, ha sido constante durante las últimas décadas, e incluso siglos, aunque ahora dispongan de instrumentos mucho más eficaces para controlar. Sin embargo, lo novedoso que nos traen las tecnologías de la información es que, en estos últimos lustros, la amenaza procede de las corporaciones privadas; en este sentido, nuestra reacción como profesionales de la información no es predecir el futuro, sino proporcionar los argumentos para promover un debate equilibrado entre personas libres.

En efecto, frente a la amenaza a la privacidad que surge del Estado, la recopilación de datos para fines privados, generalmente comerciales, tiene la particularidad de que se

originan en controles, sensores y otros herramientas que los individuos, la mayoría de las veces, no son conscientes de haber utilizado para ese propósito y de que, además, del lado de quienes los recopilan, sus autores, muchas veces no saben ni siquiera para qué los van a utilizar, ni dónde, ni cuándo. En la *Figura 1* se muestra cómo Google inserta varios anuncios publicitarios en el mensaje personal de un correo electrónico de Gmail alusivo a una boda.

Figura 1
Publicidad en mensajes privados

En el ámbito privado, tradicionalmente, el control de los individuos se ejercía desde tres focos (el director espiritual, el notario y la oficina bancaria), reflejo de los tres aspectos sociales más sensibles: la vida de las ideas, el ámbito de las decisiones privadas y el de la liquidez financiera. Hoy en día, en una sociedad en red y saturada de herramientas de producción y registro de datos (video-vigilancia, sistemas de gestión de identidad, cookies, etcétera), el beneficiario

último de esta superproducción de datos –fácilmente procesables y transmisibles– son las empresas de todo tipo, pero en especial las que se mueven en entornos donde es barata la captación de esos datos y son capaces de explotarlos en sus líneas de negocio mediante dispositivos que usan complejos algoritmos, correlacionan datos y plantean escenarios predictivos.

Un reciente informe de la consultora McKinsey cifra en tres billones de dólares el valor anual mundial de los datos abiertos, sólo en siete sectores económicos (el mayor de todos, el educativo); es importante decir que los consumidores participan en la creación de la mitad de ese valor.

No se debe olvidar que estamos en los comienzos de esta eclosión de los datos, por lo que es de esperar que cada vez más compañías se incorporen y, además, perfeccionen sus herramientas de gestión de los datos. En este sentido, ya hay experiencias realmente escandalosas que no se deben dejar de citar, como la del padre de una jovencita que se sorprende por la recepción en su casa de objetos para bebés, antes de haber llegado a advertir la sorpresa de un embarazo juvenil (Mayer-Schönberger y Cukier, 2013: p. 75 y ss).[4]

La sofisticación con la que se elaboran estas promociones comerciales nos pone sobre la pista de manipulaciones que la sociedad no debe permitir. Además, es curioso, nos

4 Resulta muy reveladora la descripción que hace el libro de esta historia. Al parecer, el embarazo hace cambiar los hábitos de compra, por lo que el equipo de la empresa de márketing examinó el historial de compras de las mujeres que se habían apuntado en su registro de regalos para bebés y en el análisis de los datos identificaron algunos productos que permitían calcular una "predicción de embarazo". A partir de estos hechos, lo anecdótico es que un padre llamó a esa empresa para quejarse de que al correo de su hija adolescente le enviaban cupones de ropa premamá. Cuando el director le devolvió la llamada unos días después, el hombre ya había descubierto que su hija estaba embarazada. Una historia demoledora que muestra el poder de los datos masivos.

recuerdan otras acciones de manipulación de masas, como las de Bernays para añadir a las mujeres a la masa de fumadores, o las actividades y experimentos más cruentos provocados por los movimientos totalitarios en la primera parte del siglo XX. La diferencia ahora es que el objetivo es cada persona concreta. Como sugiere Jaron Lanier (2014), no podemos sucumbir a la amenaza de que una futura generación electrónica de consumo tome la forma de un parche en la nuca, el cual identifica que estamos a punto de decidir a qué cafetería iremos o cuál será nuestra próxima lectura.

Tipos de datos personales

El uso de datos personales por terceros exige el consentimiento del interesado, salvo que se trate de datos anonimizados. Los datos identificables son los que tienen vinculación con la filiación de una persona, como el nombre, el número de identificación personal, el número de historial clínico, el número de la seguridad social. El problema está en que generalmente se usan datos secundarios derivados de datos personales, y en esos casos resulta importante cómo se relacionan y se disocian ambos. Los datos especialmente protegidos son los que hacen referencia al origen racial, a la salud y a la vida sexual, los cuales sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

Datos anonimizados y datos codificados

Hay dos formas de disociación de los datos personales. Por un lado, los datos anonimizados son datos personales que

han sido sometidos a un tratamiento de disociación para eliminación de datos personales. Es el caso, por ejemplo, de las sentencias o resoluciones judiciales que se publican para conocimiento general; de ahí que no se consideran datos personales. La anonimización es un proceso irreversible y, a partir de ahí, los datos dejan de ser personales.

Por el contrario, la codificación puede hacer reversible la integración de los datos personales. En este sentido, es interesante la definición que se da en la Ley española de Investigaciones Biomédicas (L 14/2007): "Dato codificado o reversiblemente disociado: dato no asociado a una persona identificada o identificable por haberse sustituido o desligado la información que identifica a esa persona utilizando un código que permita la operación inversa."

Como se ha dicho, en los casos de registros anónimos o anonimizados, no es preciso el consentimiento del afectado porque la codificación de la identidad del sujeto se ha perdido definitivamente. No es el caso de la codificación, en la que se mantiene la identidad del sujeto en un segundo plano.

Hay distintas formas particulares de codificación. Por un lado, el cifrado supone codificar la información utilizando una clave, de forma que la información resulte ininteligible sin la clave, y ésta es el factor crítico para proteger la información. Por otro, la fragmentación es un método alternativo que supone dividir la información relativa a un mismo sujeto en partes pequeñas de forma no inteligible y almacenadas en forma disjunta para evitar que los datos sean desvelados.

Computación en la nube

Mención aparte merece el tratamiento de datos personales en el modelo de *cloud computing* (computación en la

nube), lo que hace posible que tanto los proveedores de servicios como los datos almacenados en la nube se encuentren ubicados en cualquier punto del planeta. Este tipo de datos se generan de forma característica en el uso de las redes sociales, proveedores de servicios de Internet y grandes corporaciones de ámbito mundial, propio de lo que llamamos *Big data* (*Figura 2*). La computación en la nube ofrece una problemática muy amplia en diversos aspectos (para el proveedor del servicio de Internet, los usuarios, el control de los datos, la contratación de servicios con empresas y gobiernos, etcétera), así como en el tratamiento de los datos personales (García Sánchez, 2012). Pero, en todo caso, en lo concerniente a los datos personales en la nube, en esta misma obra (Martínez Martínez R., 2012) se dan algunas recomendaciones, de las que destacamos las siguientes:

- El autorizado al tratamiento de los datos es el responsable de los datos, por lo que la normativa aplicable al cliente y al prestador del servicio es la legislación propia (española/europea).
- Esta legislación no puede modificarse contractualmente.
- Aunque le informen que los datos personales están disociados, no cambia la ley aplicable ni la responsabilidad del cliente y del prestador del servicio.
- Debe evaluar la tipología de datos que trata atendiendo a su mayor o menor sensibilidad (por ejemplo, los datos meramente identificativos no son datos sensibles; en cambio, los relacionados con la salud, la ideología, o la raza, tienen la máxima sensibilidad).
- Debe informarse sobre los tipos de nube (privada, pública, híbrida) y las distintas modalidades de servicios.
- Con esta información debe decidir para qué datos personales contratará servicios de *cloud computing* y cuá-

les prefiere mantener en sus propios sistemas de información. Esta decisión es importante porque delimitará las finalidades para las que el proveedor de *cloud* puede tratar los datos. En consecuencia, debe garantizarse expresamente que no utilizará los datos para otra finalidad que no tenga relación con los servicios contratados.

Figura 2
Datos personales masivos en la nube

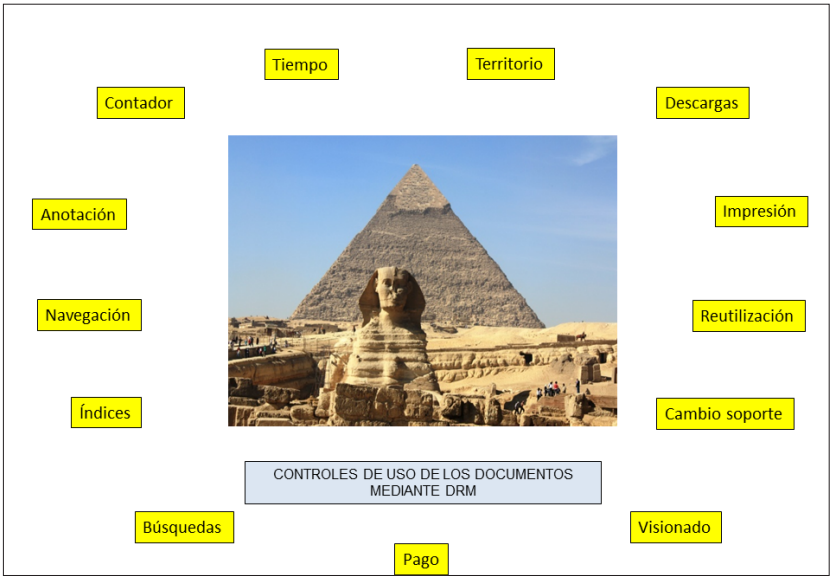
Fuente: *Vanguardia Dossier*, "El poder de las redes sociales", núm. 50, ene.-mar., 2014

En nuestro ámbito, servicios como las bibliotecas y las librerías, especialmente en línea, manejan una abundante cantidad de datos personales con un amplio uso de la computación en la nube, por lo que es importante hacer una breve reflexión sobre sus implicaciones particulares.

Es cierto que la gestión libraria no se inserta claramente ni en actividades de seguridad pública ni en tareas comerciales, ya que las bibliotecas constituyen un punto de encuentro de los valores personales y sociales, lo que no impide que sus datos sean objeto de deseo tanto desde el mundo de las ideas como de los valores económicos. Si nos centramos en cómo se gestionan los datos personales en este

entorno, enseguida concluimos que hay demasiado interés en captar todos los datos posibles, más de los necesarios, sobre la transacción entre la institución y lector. Esta avidez por los datos resulta tanto de la importancia de la lectura (para integrar gustos, autores, temas, en los estudios de mercado) como del interés por proteger los derechos de autor, lo que muchas veces se traduce en una lesión de la protección de los datos personales y su posterior uso en actividades no consentidas; es la conocida presión de los DRM, la gestión de los derechos digitales. Si se observa la *Figura 3*, la mayoría de los datos que se captan en una transacción electrónica de un libro electrónico no son necesarios para garantizar el uso legal del libro ni para asegurar el pago de la obra. Lo mismo puede aplicarse a gran parte de otros materiales culturales (películas, música, etcétera) que se gestionan en línea.

Figura 3
Controles de datos personales en los documentos gestionados con DRM



Los datos personales como recurso económico

Quienes valoran la riqueza económica que aportan los datos dicen que, ahora, éstos son lo mismo que el petróleo a la economía industrial; los datos son "[…] el recurso esencial que alimenta las innovaciones que usa la gente." (Mayer-Schönberger y Cukier, 2013, p. 224) Estos autores, vinculados a la Universidad de Oxford, sorprenden con la idea de que hay que salvaguardar unos mercados de datos masivos competitivos; de ahí que sean partidarios tanto de la implantación de una regulación antimonopolio como de que los gobiernos deben abrir sus datos. Sin dejar de reconocer "[…] los peligros de esa poderosa tecnología", proponen una solución para lograr una gobernanza justa en el manejo de los datos masivos: tres estrategias, y las tres afectan a la privacidad:

- Desplazar la protección de la privacidad desde el consentimiento individual a la responsabilidad del usuario de los datos. Frente a la idea tradicional de que sea el individuo quien controle y decida quién usa sus datos, abogan por que esta responsabilidad recaiga en los usuarios de los datos; así, serían las firmas quienes valorasen una reutilización determinada de los datos, basada en la valoración de la reutilización que efectúen, de acuerdo con unas categorías amplias de uso. Para las iniciativas de mayor riesgo, los legisladores establecerían unas reglas básicas para mitigar o evitar los daños potenciales. Este principio tendría la ventaja de estimular la creatividad y evitaría la petición del consentimiento para usos secundarios de los datos personales, de modo que un uso abusivo de los datos expondría al usuario a responsabilidades legales.

- Consagrar la voluntad humana frente a las predicciones es la segunda de estas estrategias. Aborda la forma en la que se utilizan los datos personales en la actualidad, para impedir que las predicciones se impongan a la voluntad real. Frente al riesgo de decidir sobre los datos masivos (por ejemplo, si darnos un empleo o concedernos un préstamo), los autores abogan por que se utilicen salvaguardias que garanticen la transparencia sobre los datos y el algoritmo empleado; la certificación de una tercera parte que valide el algoritmo en determinados usos sensibles, y un tercer requisito, que es la refutabilidad, de modo que las personas puedan oponerse. Con estos tres requisitos se garantizaría el libre albedrío humano, puesto que con el uso de datos masivos se corre el peligro de sustituir el comportamiento real por las predicciones basadas en los datos.
- La tercera estrategia es crear una nueva casta de auditores de datos masivos (algoritmistas). Los datos masivos precisarán de nuevos profesionales que respondan a las situaciones complejas que plantean los datos masivos que actuarían como revisores de análisis y predicciones de datos masivos, evaluando las fuentes de datos y las herramientas analíticas, a semejanza del papel que hacen los auditores en la información financiera.

Algunas estrategias, en particular la primera, chocan de plano con los principios europeos de protección de datos, en nada partidarios de hacer una cesión legal de los datos personales. Sobre los otros dos puntos, en cuanto suponen un refuerzo de la voluntad del titular de los datos o reflejan la voluntad de crear en las organizaciones un responsable de los datos, es probable que gocen de un favor más generalizado.

Conclusión: el reto de gestionar la información y favorecer la autonomía de los ciudadanos

El reto futuro es cómo gestionar la información y favorecer la autonomía de los ciudadanos. En este punto hay dos aspectos fundamentales. Por un lado, la seguridad personal (los datos que recopila el Estado para garantizar nuestra seguridad frente al terrorismo, el cibercrimen, etcétera). Por otro lado, está el uso que hacen las compañías de nuestros datos que si bien favorecen el comercio y potencian las relaciones sociales, también conllevan graves riesgos a la privacidad y a la autonomía personal.

La primera de estas cuestiones remite a que la seguridad del Estado debe estar sometido al control y a la transparencia de acuerdo al sistema de división de poderes. No hay que olvidar el hecho de que históricamente ha sido el Estado el gran recopilador de información sobre las personas, por lo que ya tenemos cierta experiencia en la gestión de esta información y del control de quienes la manejan, aunque cada día surjan nuevos retos.

El uso de los datos en el sector social es la gran revolución a la que nos enfrentamos, y son ahora las entidades privadas, con el control de las grandes redes sociales y los complejos sistemas de análisis de datos predictivos, quienes suponen una mayor amenaza cotidiana en la salvaguarda de la autonomía personal.

Caben varias opciones para gestionar la información personal, pero, desde la universidad, la única que podemos defender es la que consiste en fomentar que el individuo sepa decidir libremente con base en unos valores democráticos y en la educación adquirida, donde las bibliotecas y otras instituciones financiadas con fondos públicos favorezcan la interacción social y la comunicación entre individuos

que elijan libremente, sin la interferencia de máquinas o algoritmos que condicionen su libre albedrio, a la vez que unas instituciones públicas transparentes garantizan nuestra privacidad. Sólo así evitaremos que atrapen nuestros datos, unas veces, los grupos poderosos y, otras, personajes incompetentes, tan peligrosos los unos como los otros.

Referencias bibliográficas

Bennett, C. J. y Parsons, C. (2013). "Privacy and surveillance: The multidisciplinary literature on the capture, use and disclosure of personal information cyberspace", en Dutton, W. H. (Ed.), *The Oxford handbook of Internet studies*, Oxford, Oxford University Press.

Escalante Gonzalbo, F. (2012), *El Derecho a la privacidad*, México, IFAI.

García Sánchez, M. (2012), "Retos de la computación en nube", en Martínez Martínez, R. (Ed.), *Derecho y Cloud Computing*, Pamplona, Civitas.

IFLA Trend Report (2013), *¿Surcando las olas o atrapados por la marea? Navegando el entorno en evolución de la información* [en línea], http://trends.ifla.org/files/trends/assets/surcando_las_olas_o_atrapados_en_la_marea.pdf (consultado 20-2-2014).

Lanier, J. (2014), "Nuevas concepciones de la privacidad", en *Investigación y Ciencia* (448), enero, 53-59.

Martínez Martínez, R. (Ed.) (2012), *Derecho y Clod Computing*, Pamplona, Civitas.

Martínez Martínez, R. (2007), "El derecho fundamental a la protección de datos: perspectivas", Monográfico: III Congreso Internet, Derecho y Política, en *IDP. Revista de Internet, Derecho y Política* [en línea], file:///D:/Downloads/Dialnet-ElDerecho-FundamentalALaProteccionDeDatosPerspectiv-2372613.pdf

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

Prost, F. (1993), "Fronteras y espacio de lo público", en Aries, P., y Duby, G. (Coord.), *Historia de la vida privada* [Tom. 5. De la Primera Guerra Mundial a nuestros días], Barcelona, Círculo de Lectores.

The McKinsey&Company (2013), "Open data: Unlocking innovation and performance with liquid information" [en línea], http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information