DERECHOS HUMANOS EMERGENTES
Y PERIODISMO

PLIEGOS DE INFORMACIÓN es una
Colección Bibliográfica del
EQUIPO DE INVESTIGACIÓN DE ANÁLISIS
Y TÉCNICA DE LA INFORMACIÓN,
de la Universidad de Sevilla
y adscrito al Departamento de Periodismo II.

Edición realizada con las colaboraciones de:

UNIVERSIDAD DE SEVILLA
VICERRECTORADO DE
RELACIONES INSTITUCIONALES.

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA,
INNOVACIÓN, CIENCIA Y EMPLEO

Capítulo 29

El derecho a la protección de los datos personales en los entornos cibernéticos: entre la privacidad y la Publicidad

Noelia García Estévez [*]

1. INTRODUCCIÓN.

Con la llegada de las tecnologías de la información y la comunicación a diversos ámbitos de la vida económica y social, y dada la creciente importancia y poder del procesamiento informatizado de datos, es necesario realizar un análisis exhaustivo de cómo los datos de carácter personal del ciudadano de hoy están siendo recopilados, tratados y utilizados con diferentes fines. En este artículo nos centramos, sobre todo, en el uso publicitario de estos datos y, más concretamente en dos aspectos clave de esta encrucijada: en cómo la publicidad y las empresas anunciantes están utilizando esta macro-cantidad de datos con el fin de hacer más relevante y eficaz su mensaje comercial, por un lado, y qué riesgos o mermas pueden tener estas prácticas ante la privacidad y la salvaguardia de los datos personales de los usuarios.

Con la creciente participación del ciudadano en Internet y sus múltiples interacciones en los entornos digitales se va dejando un rastro digital que permite configurar un perfil exhaustivo del usuario y conocer los comportamientos, gustos, aficiones, necesidades… Esto supone un estupendo 'caldo de cultivo' para desarrollar una eficaz segmentación necesaria para la publicidad comportamental. Existe una diversidad de aproximaciones al concepto de publicidad comportamental, si bien nosotros nos basaremos en la ofrecida por Pérez Bes (2012: 13):

[*] Profesora en el Centro Universitario San Isidoro-CEADE, de Sevilla, y en la Universidad de la misma ciudad, España.

> "[…] lo que caracteriza a la publicidad comportamental no debe ser la elección de una u otra publicidad basada en la conducta del consumidor, sino la utilización de técnicas de segmentación que permiten a un tercero analizar el comportamiento y las características de un usuario a través de sus acciones y hábitos de navegación (frecuencia de visitas a sitios concretos, interacciones, búsquedas de palabras clave, cliks en determinada publicidad, tiempo de permanencia en ciertos contenidos, etc.) con tal de desarrollar un perfil en base al cual se pueda dirigir publicidad que resulte acorde con esos presumibles intereses inferidos de su conducta online".

Sin duda, este tipo de publicidad tiene ciertas ventajas tanto para los anunciantes como para los receptores de la misma. No obstante, se nos plantea un dilema en el que se implican aspectos tanto legales como morales. Estamos de acuerdo con López y Martínez (2010) que "aunque la publicidad comportamental puede aportar ciertas ventajas tanto a la industria como al usuario, debe valorarse la invasión de la privacidad que tal forma publicitaria puede representar".

Son muchas y muy diversas las maneras en las que se recopilan información y datos de diferente índole de los usuarios mientras navegan por Internet. Según Emilio Suñé (2002), director del Máster en Informática y Derecho de la Universidad Complutense de Madrid, las principales tecnologías de control de la información y de los datos personales en los entornos cibernéticos son las siguientes:

> * Las *cookies*. Son ficheros de datos que determinados servidores envían a los ordenadores que se conectan a sus páginas web, quedando almacenados en el disco duro. Así, cada vez que un usuario visita estas páginas web, la cookie almacenada es reenviada al servidor, proporcionándole una amplia gama de información entre la que se incluyen datos personales: la dirección IP; datos sobre el software y el hardware; a veces, incluso, la dirección email y la contraseña; registro de las secciones de la website visitada; etc.
>
> * Rastros de cliqueo o *clickstream*. Son los clics del ratón o los datos introducidos a través del teclado que realizan los usuarios de Internet en sus actividades quedando constancia del comportamiento, las elecciones y las preferencias que ha manifestado una persona al visitar determinados sitios web.

* Acumulación innecesaria de datos. El almacenamiento sistemático de datos para su posterior minería, es posible en razón de su bajo coste, combinado con su extrema utilidad, que para las empresas se traduce en la posibilidad de elaborar perfiles personales, para explotarlos en función de sus intereses. Todo ello está relacionado con las técnicas de *data mining*.

* Procesadores no anónimos de acceso a la red. Se trata del deseo y la voluntad de las empresas que comercializan sistemas operativos de controlar los procesadores y sus usuarios. Intel lo intentó con los procesadores Pentiun III y así lo anunció aunque finalmente no lo hizo por la presión de los internautas.

* Transmisiones de datos por el propio interesado, que escapan a su control. Se refiere a todos los datos que los usuarios transfieren cuando deciden participar en un servicio de correo electrónico, plataforma social, foro de discusión… Son, al fin y al cabo, los términos y condiciones que se aceptan voluntariamente pero en gran cantidad de ocasiones de manera inconsciente y "obligada", si se quiere disfrutar de ese servicio.

* Motores de búsqueda. Los motores de búsqueda también pueden ser utilizados para encontrar datos personales en Internet. Además, a través de las búsquedas realizadas, los servidores de los motores de búsqueda tienen la posibilidad de establecer, a su vez, perfiles personales.

* Otras tecnologías invasivas de la intimidad.

2. HACÍA UNA DEFINICIÓN DE DATOS PERSONALES Y SU PROTECCIÓN EN INTERNET.

Se entiende que el derecho a la protección de datos es el derecho que tiene todo ciudadano a controlar sus datos personales y decidir sobre los mismos. Existen diferentes normativas y leyes que intentan regular y garantizar este derecho. Así, por ejemplo, a nivel europeo nos encontramos con la Directiva 95/46/CE (Unión Europea, 1995), que es la norma de referencia en materia de protección de datos. De acuerdo con la definición que contiene la Directiva 95/46/CE, "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número

de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

La citada Directiva 95/46/CE, indica en su considerando 26 que: "[...] para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta […] pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado".

En el caso español hallamos la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) (España, 1999) y su Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal (RDLOPD) (España, 2008) que conforman las bases legales para la protección de los datos de los ciudadanos. Estas leyes se desarrollan fundamentándose en el artículo 18 de la constitución española de 1978, sobre el derecho a la intimidad familiar y personal y el secreto de las comunicaciones.

La LOPD define 'dato de carácter personal' en su artículo 3 como "cualquier información concerniente a personas físicas identificadas o identificables". La RDLOPD, por su parte, entiende que dato de carácter personal es "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier tipo concernientes a personas físicas identificadas o identificables". Esta normativa sobre protección establece una serie de derechos a los sujetos titulares de los datos como son:

* Derecho de acceso, según el cual el ciudadano puede solicitar y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, así como el origen de dichos datos y las comunicaciones realizadas o que se prevean realizar.

* Derecho de rectificación, que permite que un ciudadano se dirija al responsable de un fichero o tratamiento para que rectifique sus datos personales.

* Derecho de cancelación, que da la posibilidad de dirigirse al responsable para solicitar la cancelación de sus datos personales.

* Derecho de oposición, por el cual un ciudadano puede oponerse a que sus datos sean tratados con fines de publicidad y de protección comercial.

Internet es un fenómeno global y, en ocasiones, no basta con las legislaciones nacionales particulares y es necesario establecer patrones internacionales que garanticen la seguridad y protección de los ciudadanos más allá de las fronteras de un país en cuestión. Es por ello que en el año 2002 vieron la luz las "Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales" con el fin de adaptar e implantar las "Directrices sobre la protección de la privacidad y flujos transfronterizos de datos personales" de 1980 a la nueva coyuntura del siglo XXI protagonizada por un rápido y generalizado desarrollo de tecnologías e infraestructuras de información y comunicaciones y el vertiginoso avance hacia una sociedad global de la informaciones. En este informe la OCDE (2002) reconoce que:

> "Los países miembros de la OCDE se han comprometido por entero a proteger la privacidad en el ámbito global, cooperando activamente con la empresa y la industria, la sociedad civil, los países no pertenecientes a la OCDE y otras organizaciones internacionales, para valorar las tendencias económicas y tecnológicas clave que puedan afectar a la privacidad, desarrollando políticas exhaustivas y coherentes".

En la primera parte de estas directrices se ofrece una definición de 'datos personales' muy parecida a la de la LOPD, delimitando que "son cualquier información relacionada con un individuo identificado o identificable (sujeto de los datos)". No obstante, y a pesar de la delimitación del concepto de dato de carácter personal propuesto por estas leyes y directrices, existen ciertos vacíos o aspectos dilemáticos cuando aplicamos este concepto en los entornos cibernéticos y/o digitales.

Para Red Bull (2015), en sus "Directrices de protección de datos y privacidad", los datos personales son las informaciones reales como el nombre, la dirección postal, el número de teléfono, o la dirección de correo electrónico y dirección IP completa. Sin embargo, las informaciones que no permiten conocer la identidad de una persona, como por ejemplo la cantidad de usuarios de un sitio web, el tiempo de permanencia en un sitio y los enlaces utilizados en un sitio web no son datos personales.

3. LA CESIÓN DE LOS DATOS PERSONALES Y LA PROPIA PRIVACIDAD EN LAS PLATAFORMAS SOCIALES ONLINE.

Decía Lorena Fernández, impulsora del uso de las TIC y la web 2.0 en la docencia en la Universidad de Deusto y autora de un prestigioso blog[1], en una entrevista concedida a *El País* (2009) que "las redes son servicios gratuitos, pero tienen una contraprestación: los datos de los usuarios" . Quizá sea acertado pensar que todas las posibilidades que nos ofrecen estos sitios sociales tiene un precio y que éste sea precisamente algo tan delicado como nuestra privacidad. La privacidad como tal, afirma Dans (2010: 224), empieza a ser "una anomalía histórica".

La salvaguardia de nuestra identidad tiene en las redes sociales diversas vertientes: por un lado, la protección de Datos de Carácter Personal; por otro, la protección de la Privacidad, Honor, Intimidad y Propia Imagen; y, por último, la protección de la Propiedad Intelectual e Industrial.

En primer lugar, cuando un individuo se da de alta en una plataforma de servicios de red social acepta una serie de condiciones entre las que se establece el uso que este sitio podrá hacer de los datos personales de sus miembros. Es importante leer detenidamente estas condiciones que, por su parte, suelen ser muy extensas y con un lenguaje algo farragoso[2]. De forma que la mayoría de los usuarios no lee los avisos legales y políticas de privacidad y, en aquellos casos en los que son revisados por los usuarios, no son realmente comprendidos. No obstante, muchos sitios de redes sociales han reescrito sus políticas de privacidad con el fin de hacerlas más inteligibles al ciudadano medio.

Los primeros datos básicos que suelen solicitarse a la hora de abrir una cuenta en una red social son el nombre, correo electrónico, sexo y fecha de nacimiento. Luego es el usuario quien va proporcionando el resto de información, a través de su perfil y sus interacciones en la red. En el año 2010 en la Política de Privacidad de Facebook, la red social más popular en el

[1] Puede conocerse en: <http://blog.loretahur.net/>. [Consulta: 14/01/2015].

[2] La Agencia Española de Protección de Datos (AEPD) en su "Informe sobre buscadores de Internet", publicado el día 1 de diciembre de 2007, establecía la necesidad y la obligación por parte de los prestadores de servicios de la Sociedad de la Información, de facilitar a los usuarios una información real y efectiva respecto al cumplimiento de las obligaciones legalmente dispuestas. Véase en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/declaracion_aepd_buscadores.pdf>. [Consulta: 02/01/2015].

mundo, se decía claramente que el servicio permitía a sus usuarios actualizar su estado, cargar o hacer fotos, cargar o grabar vídeos, compartir un enlace, crear un evento o un grupo, hacer un comentario, escribir algo en el muro de alguien, escribir una nota o enviar un mensaje. Si el usuario no desea que Facebook guarde "los metadatos asociados al contenido que compartes en Facebook (como las fotografías) elimina los metadatos antes de cargar el contenido". En la última versión de dicha política, hoy denominada Política de datos, de enero de 2015 nos sigue informando del tipo de información que Facebook recopila pero comprobamos como no deja opción para que el usuario pueda evitarlo.

De hecho, si comparamos las políticas de 2010 con la de 2015, observamos que la red social de Zuckerberg cada vez recopila más información y deja menos opciones a la privacidad del usuario. Así, hace cinco años Facebook guardaba los datos de las transacciones o pagos que sus miembros realizan a través de la plataforma. Pero nuevamente, si no se deseaba que se almacenara el número de cuenta de origen del pago, el usuario debía eliminarlo a través de la página de pagos. En la actualidad Facebook almacena "información del pago, como el número de tu tarjeta de crédito o de débito y otra información sobre la tarjeta, así como otros datos sobre la cuenta y la autenticación, además de detalles de facturación, de envío y de contacto", sin opción a poder evitarlo.

Cada vez que un usuario interactúa en esta red social, Facebook va recopilando información que utilizará con diferentes objetivos: desde mejorar el servicio hasta ofrecer perfiles de target más completos a empresas anunciantes. Así, esta red social realiza un seguimiento de las acciones que un usuario lleva a cabo en Facebook, como añadir conexiones (incluido unirse a un grupo o añadir un amigo), crear un álbum de fotos, indicar un "me gusta" a una publicación, asistir a un evento o conectarse a una aplicación.

Además, Facebook puede también obtener información sobre los dispositivos y navegadores desde los cuales se conectan sus usuarios, como la ubicación, la dirección IP o las páginas que visitan. El uso de *cookies* es también habitual para, argumentan desde la corporación, "proporcionar y mantener nuestros Servicios y cada uno de los usos mencionados y descritos en esta sección de nuestra política" (Facebook, 2015a).

En cuanto a la información recopilada y cesada con fines publicitarios, Facebook dice pretender publicar anuncios y otro contenido comercial o patrocinado que sea valioso para sus usuarios y anunciantes. De este modo, cada usuario de esta red social acepta las siguientes condiciones según sus términos legales (Facebook, 2015b):

> "1. Nos concedes permiso para usar tu nombre, foto del perfil, contenido e información en relación con contenido comercial, patrocinado o asociado (como una marca que te guste) que publiquemos u optimicemos. Esto significa, por ejemplo, que permites que una empresa u otra entidad nos pague por mostrar tu nombre y/o foto del perfil con tu contenido o información sin que recibas ninguna compensación por ello. Si seleccionaste un público específico para tu contenido o información, respetaremos tu elección cuando lo usemos.
>
> 2. No proporcionamos tu contenido o información a anunciantes sin tu consentimiento.
>
> 3. Entiendes que es posible que no siempre identifiquemos las comunicaciones y los servicios de pago como tales".

En la Política de datos (Facebook, 2015a) también se expresa que esta red social tiene el objetivo de mostrar una publicidad "relevante e interesante" para el usuario, por lo que esta plataforma usa toda la información que tiene acerca de cada uno para mostrar "anuncios relevantes". Asegura no compartir información que identifique de forma personal al usuario (es decir, información, como el nombre o dirección de correo electrónico) con socios que prestan servicios de publicidad, medición o análisis, a menos que el usuario nos de su permiso (Facebook, 2015a).

Como vemos, encontramos ciertas incongruencias y/o discrepancias entre el Acuerdo de los términos legales y la Política de Datos pues, según el primero, Facebook sí puede mostrar el nombre del usuario a otra empresa o entidad mientras que en la Política de Datos afirman no compartir información que identifique a la persona, como su nombre.

El desarrollo de Open Graph como la nueva API de Facebook desde abril de 2010 generó cierta polémica en torno a la utilización indiscriminada de información de los usuarios. Esta herramienta permite que en los sitios web externos a la plataforma se integren funciones sociales propias de Facebook mediante sencillos *widgets*. Pero además, permite que Facebook recopile la información de los usuarios en éstas, algo que ciertos analistas han considerado una violación del derecho a la intimidad. Incluso cuatro senadores de los Estados Unidos escribieron una carta al máximo responsable de Facebook, Mark Zuckerberg, exigiendo a la compañía que revise su sistema de personalización instantánea que permite compartir perfiles de Facebook en otros sitios de Internet.

De hecho, en aquel momento hubo una oleada de críticas en torno a los criterios de privacidad de Facebook, aunque ello no ha impidió que cada mes aumentara considerablemente el número de usuarios. Las palabras del fundador y CEO de Facebook, Mark Zuckerberg, en una entrevista con Michael Arrington con Techcrunch[3] en la que afirmó que ha afirmó que "la era de la privacidad ha acabado" y que si tuviera que volver a crear la red social los datos de los usuarios serían totalmente públicos, crispó aún más el asunto. Surgieron así grupos de internautas en contra de Facebook, uno de los más radicales, "We'Re Quitting Faceboob" (s. a.), proponía abandonar definitivamente el 31 de mayo de 2010 esta red social, cosa que, como sabemos, no sucedió.

Comprobamos como existen muchos y delicados aspectos relacionados con la (des)protección de nuestros datos personales en Internet. Es más, recuperamos otro fragmento incluido en el Acuerdo de términos legales (Facebook, 2015b) en su punto 15 en el que se advierte en mayúscula que de que las medidas de seguridad pueden ser burladas sin tener la compañía ninguna responsabilidad:

> "Intentamos mantener Facebook en funcionamiento, sin errores y seguro, pero […] no garantizamos que Facebook sea siempre seguro o esté libre de errores, ni que funcione siempre sin interrupciones, retrasos o imperfecciones. Facebook no se responsabiliza de las acciones, el contenido, la información o los datos de terceros, y por la presente nos dispensas a nosotros, nuestros directivos, empleados y agentes de cualquier demanda o daños, conocidos o desconocidos, derivados de cualquier demanda que tengas interpuesta contra tales terceros o de algún modo relacionados con esta […]".

En tales circunstancias, no nos extraña que la preocupación general por proteger la intimidad de los usuarios de las redes sociales en Internet. El propio concepto de red social conlleva la renuncia por parte de los usuarios de cierta parte de ese derecho fundamental. Para la protección de la privacidad y el derecho al honor es clave la autoconciencia del usuario con respecto a su propia intimidad y con la de los demás. Existen tres momentos claves en la configuración de la privacidad de un usuario de un sitio de redes sociales online: el alta, la participación y la baja. El primero de ellos parte del momento de registro de alta como usuario. Es importante conocer los sistemas y criterios

[3] La entrevista, de una duración de seis minutos en la que Zuckerberg sólo utilizó sesenta segundos para hablar de la política de privacidad de Facebook, puede verse a través de la red. Véase <https://www.youtube.com/watch?v=LoWKGBloMsU>. [Consulta: 14/01/2015].

de privacidad que ofrece cada plataforma, con el fin de configurar correctamente el nivel de privacidad del perfil y limitar el acceso de terceros a nuestros datos personales. Cuando se participa en la red el usuario ha de utilizar criterios de lógica y sentido común en cuanto a la cantidad de información que publica, datos e imágenes que puedan afectar a la privacidad, tanto personal como de terceros. En el instante que un usuario solicita darse de baja de la plataforma, es posible que gran parte de sus datos continúen alojados en el servidor y que tarde un periodo más o menos largo hasta que desaparezcan por completo. A veces los datos de carácter personal y la información íntima del usuario continua publicada y es accesible desde los perfiles de otros usuarios e indexada y almacenada en la caché de los distintos buscadores existentes en Internet.

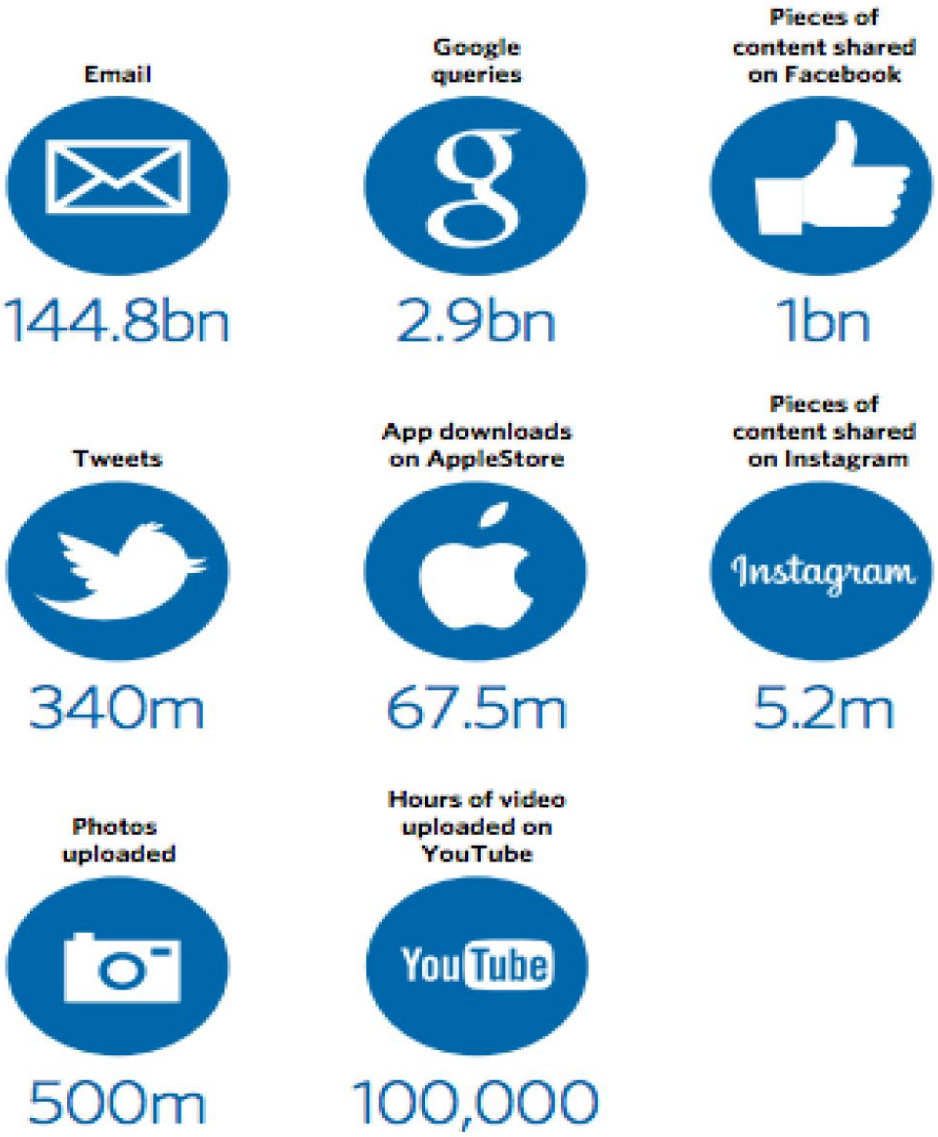
4. EL IMPACTO DE BIG DATA COMO ESTRATEGIA COMERCIAL.

Para entender la coyuntura del panorama actual y la creciente relevancia de los datos personales que circulan en la red, hemos de repasar y repensar algunas cifras que ponen de manifiesto este hecho. El motor de búsqueda Google, por ejemplo, procesa más de 24 petabytes de datos al día; a la red social Facebook, una de las más importantes del mundo, se suben más de diez millones de fotos nuevas cada hora y sus usuarios hacen clic en el botón de "me gusta" o insertan un comentario casi tres mil millones de veces diarias, dejan un valioso rastro digital; en Youtube se sube más de una hora de vídeo cada segundo; el número de mensajes de Twitter aumenta alrededor de un doscientos por cien… (Mayer-Schönberger y Cukier, 2013: 19).

El informe de European Voice "Data: The New Currency?" (2014) establece una distinción entre 'datos masivos' y 'big data'. Los primeros se refieren a las grandes cantidades de información electrónica que puede requerir grandes ordenadores para manejar el procesamiento debido a su tamaño. En términos de formato, los datos masivos pueden ser considerados como el equivalente a las hojas de cálculo. Por su parte, en el caso de big data la información se obtiene de una amplia gama de fuentes en una variedad de formatos. Una de las características de big data es que se basa en la mezcla de diferentes conjuntos de datos con el fin de generar valor.

Según este informe, el 90% de los datos se han producido en los últimos años. En la "Ilustración 1" se puede observar una infografía que representa en cifras la manera tan extraordinaria de generación de datos por parte de los usuarios en función de las diferentes plataformas y servicios online que encontramos en Internet.

ILUSTRACION 1.
Cantidad de datos generados en un día.



Fuente: European Voice (2012).

Los datos siempre han sido importantes para el mundo empresarial y publicitario. Richard Tobaccowala, jefe de innovación del grupo Publicis Groupe Media, establecía cinco reglas clave que deben cumplir las agencias de publicidad y las fórmulas de anunciarse. La tercera de estas reglas hace alusión precisamente a la importancia de los datos en el contexto publicitario actual (Tobaccowala citado en Jarvis, 2010: 196):

> "Tercera: datos. Los anunciantes aman los datos casi tanto como Google. Ellos creen que los datos les dicen dónde gastar su dinero y el retorno que consiguen sobre la inversión. […] Es ahora cuando llega el

más medible de los medios de la historia, Internet, donde los anuncios pueden aprender más que nunca de sus clientes".

Para la empresa anunciante los datos son, en primer lugar, la manera de conocer a un cliente y ofrecerle el producto oportuno en el momento adecuado. Pero, además, después de la acción comercial los datos en Internet permiten cotejar los resultados de la acción publicitaria y extraer mediciones muy precisas. Pero para que esto sea posible se hace necesario saber sacar provecho a la gran cantidad de información que se extrae de los datos, lo que conlleva tener claro los objetivos que se pretenden y disponer de personal cualificado. En este sentido, María José Miranda, directora general de NetApp en el segmento de Iberia, entiende que todavía no se sabe aprovechar el big data "ya que no es fácil transformar esa gran cantidad de información e integrarla de forma adecuada para sacar un beneficio. Además, se requieren experto para saber qué utilidad tiene esa información y tampoco hay muchos especialista en esto" (Entrevista a Miranda en Delgado, 2015).

Este aluvión de información y las posibilidades que el big data brinda para su utilización, con diversidad de fines, nos obliga a replantearnos los principios clave de privacidad. Esa vigilancia continuada de nuestro existir en Internet, que es nuestro existir en el mundo de hoy día, pone en jaque nuestra intimidad y privacidad.

5. REFERENCIAS.

Dans. E. (2010). *Todo va a cambiar. Tecnología y evolución: adaptarse o desaparecer*. Barcelona: Deusto.

Delgado, María (2015). "'Las firmas aún no saben explotar las bases de datos' (entrevista a María José Miranda)" en *El Economista*, 12 de mayo, p. 40.

El País (2009). "La letra pequeña de la comunidad 'on-line'. ¡Socorro! ¡Quiero escapar de mi red social!" en *El País Semanal*, España, 20 de diciembre, pp. 89-90.

España (2008). "*Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*" en *BOE*, nº. 17. de 19 de enero de 2008, pp. 4103-4136.

España (1999). *"Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal"* en *BOE*, nº. 298. de 14 de diciembre de 1999, pp. 43088-43099.

European Voice (2014). *"Data: The New Currency?"* : <http://goo.gl/jVlh7P>. [Consulta: 12/01/2015].

Facebook:
* (2010). *"Política de privacidad de Facebook"*, actualizada a 22 de abril de 2010: <http://www.facebook.com/policy.php>. [Consulta: 02/01/2015].

* (2015a). *"Política de datos de Facebook"*, actualizada a 3 de enero de 2015: <https://www.facebook.com/privacy> . [Consulta: 20/01/2015].

*(2015b). *"Acuerdo de términos legales de Facebook"*, actualizado a 30 de enero de 2015: <https://www.facebook.com/legal/terms/update>. [Consulta: 01/02/2015].

Inteco (2012). *Guía para usuarios: identidad digital y reputación online*. Madrid: Ministerio de Industria, Energía y Turismo.

Jarvis, Jeff (2010). *Y Google, ¿cómo lo haría?* Barcelona: Gestión 2000.

López Jiménez, David y Martínez López, Francisco José (2010). "Nuevas coordenadas en el ámbito de la web 2.0: el caso de la publicidad comportamental" en *Revista de Estudios Económicos y Empresariales*, nº. 22, pp. 101-134.

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

OCDE (2002). *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*: <http://www.oecd.org/sti/ieconomy/15590267.pdf>. [Consulta: 08/01/2015].

Suñé, Emilio (2002). "La protección de datos personales en Internet" en *Actas del II Congreso Mundial de Derecho Informático*: <http://goo.gl/DNbuuf>. [Consulta: 14/01/2015].

Unión Europea (1995). *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas*

físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos:
<http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046>.
[Consulta: 16/11/2014].

"We'Re Quitting Faceboob" (s. a.): <http://www.quitfacebookday.com/>.
[Consulta: 25/12/2014].