



colegio oficial
ingenieros de telecomunicación

Protección de Datos y Privacidad en el Sector TIC

Panorámica sobre la problemática actual, las perspectivas futuras, así como el valor económico con respecto a la privacidad y la protección en el sector TIC

Grupo de Políticas Públicas y Regulación
Colegio Oficial de Ingenieros de Telecomunicación



colegio oficial
ingenieros de telecomunicación

Protección de datos y privacidad en el sector TIC

Coordinador

José Antonio Portilla Figueras

Juan Santaella Vallejo

Autor

Arturo Vergara Pardillo

Grupo de Políticas Públicas y Regulación
Colegio Oficial de Ingenieros de Telecomunicación



colegio oficial
ingenieros de telecomunicación

Coordinador del grupo

Julio Navío Marco

Miembros

Antonio Alcolea Muñoz
Antonio Ángel Botella Galindo
Sonia Castillo Triguero
Luis Jesús Delpon Miguel
Javier Escudero Álvarez
Javier Fernández Fraga
Eugenio Fontán Oñate
Francisco Javier Gabiola Ondarra
Francisco Javier García Rodríguez
Luis Gil Palacios
Ana Isabel Gómez Pérez
Matías González Martín
Ricardo Gutiérrez Losa
Leandro de Haro y Ariet
Ramón Lois
Benjamín López Hidalgo
José Luis Machota Vadillo
Ana de los Ángeles Marín Andreu
Jesús Martín Porras
Víctor Martín
Noelia Miranda Santos
Juan Antonio Muñoz del Castillo
Julio Navío Marco
Adrián Nogales Escudero
Dionisio Oliver Segura
José Antonio Portilla Figueras
Amador Rodríguez Toro
Juan Romeo
Juan Santaella Vallejo
Maite Tamayo Vivanco
Josep Ventosa Freixedes
Arturo Vergara Pardillo
Daniel Vicente Tóbar



Resumen Ejecutivo

La elaboración de este documento pretende proporcionar una visión panorámica sobre la situación actual y las perspectivas futuras en cuanto a la privacidad y protección de datos en el mercado TIC, pretendiendo resaltar las implicaciones económicas y sociales en cuanto a nuevas tecnologías (Cloud Computing, Big Data) y servicios (Redes Sociales).

El desarrollo de la tecnología ha facilitado la capacidad de recolección, almacenamiento y agregación de los datos. La utilización de estos por parte de las empresas les ha permitido crear nuevas oportunidades de negocio, mejorar sus servicios y aumentar sus beneficios socioeconómicos, pero la generación de estos nuevos modelos de negocios no debe de ir en detrimento de la privacidad de los usuarios, ya que existe entre la población la sensación de cierta inseguridad ante posibles “mala-praxis” en relación a la utilización de datos de carácter personal e información privada. Por lo que es necesario un marco regulatorio lo suficientemente claro, preciso y flexible para evitar crear inseguridades a los ciudadanos.

Las actuales leyes europeas de protección de datos datan de 1995, antes incluso de que Internet tuviera un uso masivo, lo que incrementa el riesgo de que la sociedad pierda el control sobre sus propios datos. Por estas razones la Comisión Europea ha presentado una propuesta para la creación de un Reglamento para Privacidad y Protección de los Datos Personales que está actualmente en proceso de tramitación en el Parlamento Europeo. En la que se pide a los Estados miembros que adopten medidas para poner fin a la violación del derecho de la privacidad en Internet; aprueben legislaciones que garanticen el cumplimiento del derecho humanitario internacional y reactiven la vigilancia sobre la recolección de datos personales, sancionando con contundencia las correspondientes acciones punibles.

En definitiva este informe pretende desarrollar las implicaciones del manejo de los datos en las tendencias actuales del sector TIC, donde el usuario cede parte de su privacidad, para mejorar los servicios ya sean ofrecidos por parte de una empresa o por la propia administración, pero en el que se deben desarrollar buenas prácticas que produzcan un incremento de la sensación de seguridad y confianza en los usuarios.

Executive Summary

This document provides an overall view of the current status and future perspectives of the issues of privacy and data protection involving ICT markets while highlighting the financial and social implications of new technologies (Cloud Computing, Big Data) and services (Social Networks).

Advances in technology have brought new capabilities such as data collection, storage and aggregation. Corporate use of such data has created new business opportunities, improved services offered and enhanced socioeconomic benefits for companies but the emergence of such new business models should not clash with user privacy as customers presently have a certain uneasy feeling about possible malpractice relative to the use of data involving personal and private information. For this reason, a new regulatory framework is necessary which is sufficiently clear, precise and flexible in order to avoid generating insecurity among citizens.

Current European data protection laws were established in 1995, before the Internet became a massive communications medium which increases the risk of having society loose control of its own data. For this reason, the European Commission has drafted a proposal for the creation of new Privacy and Data Protection Rules for personal data. This proposal is currently being processed by the European Parliament while it requests that Member States take the necessary measures to stop the infringement of Privacy Rights on the Internet as well as passing new legislation that insures compliance with international humanitarian rights while reactivating vigilance over personal data collection activities and imposing firm sanctions on punishable actions.

In short, this report strives to lay out the implications of current data management trends in the ICT sector in which each user cedes part of their privacy in order to improve services offered either by corporations or governments while these should only develop proper operating practices that lead to an increased feeling of security and confidence among end users.







Índice de Contenidos

1	INTRODUCCIÓN	13
2	EL ESCENARIO ACTUAL: GEOPOLÍTICA INTERNACIONAL	14
2.1	<i>Circunstancias Geopolíticas</i>	<i>15</i>
3	PRIVACIDAD, PROTECCIÓN DE DATOS Y TENDENCIAS TIC	19
3.1	<i>Redes Sociales: Responsabilidad Compartida</i>	<i>19</i>
3.2	<i>Cloud: Sistema y Almacenamiento en la nube.....</i>	<i>23</i>
3.3	<i>Big Data: Máximo aprovechamiento de los datos.....</i>	<i>26</i>
3.4	<i>El problema de los Call Centers</i>	<i>29</i>
4	EL FUTURO DE LA REGULACIÓN ~2016	31
5	ECONOMÍA BASADA EN DATOS.....	34
6	CONCLUSIONES	38
7	ANEXO I.....	41



1 INTRODUCCIÓN

El derecho a la **privacidad**, es decir, la existencia de un derecho personal e inviolable a preservar aquellos aspectos de uno mismo que considera privados, es un concepto que está universalmente aceptado. Actualmente, la privacidad ha saltado al primer plano de la actualidad en distintos sectores debido a que, con las nuevas tecnologías de la información y comunicaciones, han desaparecido las limitaciones inherentes a la recopilación de datos, almacenaje, agregación, análisis y transmisión de estos datos produciendo cambios significativos en el volumen y el uso de los datos personales.



Este escenario obliga al Ingeniero de Telecomunicación a adquirir ciertos conocimientos acerca de la situación actual en cuanto a la privacidad y protección de datos. El primer paso consiste en encuadrar el concepto de *Dato Personal*. La definición de la OCDE establece que "*Toda información sobre una persona física identificada o identificable individualmente*¹", por ejemplo, datos sociales, de localización o de comportamiento, entre otros. Esta definición, o cualquier otra que se pueda encontrar, se vuelven cada vez menos precisas, debido a que cada vez **resulta más difícil distinguir entre los datos personales y no personales**. Las técnicas actuales de agregación, combinación y análisis permiten que casi cualquier tipo de datos, aunque estos no sean personales, se relacionen con la verdadera identidad de una persona. Por tanto, cualquier forma de asociación entre estos datos y una identidad virtual rompe el anonimato de este último, tal y como están demostrando las técnicas de "**Big Data**".

Llegados a este punto se deben considerar dos cuestiones. La primera se centra en el propio concepto de privacidad, que se caracteriza por variar, tanto en el tiempo como en las distintas partes del mundo, e incluso entre distintas generaciones que conviven en el mismo tiempo y lugar. Por lo tanto, la idea de **privacidad es un concepto vago**, que es distinto entre Norteamérica y Europa, incluso a nivel regulatorio, y radicalmente distinto al que puede existir en Asia. Adicionalmente, se debe tener en cuenta que existe una gran diferencia en cuanto a lo que los individuos consideran como privacidad y lo que desde el punto de vista legal es el concepto de privacidad.

La segunda idea se basa en la transversalidad de los problemas relacionados con la protección de la privacidad, no siendo estos específicos del sector TIC, sino que afectan

¹ OCDE Privacy Guidelines

a diferentes sectores económicos, y a diferentes ámbitos de la vida en general. Prueba de ello es que la Directiva de Protección de Datos es de aplicación general, desde un centro médico, a una empresa de reparto a domicilio.

La utilización de los datos en general, y de los datos de carácter personal en particular, permiten a las empresas crear nuevas oportunidades de negocio, mejorar sus servicios actuales y **aumentar sus beneficios socioeconómicos**. Existen numerosos casos de éxito de aplicación, recopilación y análisis de información personal con beneficios inmediatos, por ejemplo, cuando se usan orientados a solucionar problemas de salud pública².

Sin embargo es necesario un marco regulatorio suficientemente claro, preciso y flexible para evitar crear inseguridades a los usuarios. La actual legislación básica en materia de Protección de Datos en el ámbito de la Unión Europea, debido a los cambios tecnológicos, *ha perdido actualidad* a la hora de garantizar el derecho a la privacidad de las personas físicas e incluso han aparecido discrepancias en su aplicación entre los distintos estados miembros de la Unión Europea (UE). Por estas razones la Comisión Europea ha presentado una propuesta para la creación de un Reglamento para Privacidad y Protección de los Datos Personales³ que está actualmente en proceso de tramitación en el Parlamento Europeo.

El objetivo de este documento es proporcionar una panorámica sobre la problemática actual, las perspectivas futuras, así como el valor económico de la privacidad y la protección de datos a través de su cadena de valor en el sector TIC.

2 EL ESCENARIO ACTUAL: GEOPOLÍTICA INTERNACIONAL

Actualmente existe por parte de los gobiernos, las grandes compañías privadas del sector TIC y los ciudadanos en general, una importante preocupación respecto a lo que se puede definir como "*mala-praxis*" en relación a la utilización de datos de carácter personal e información privada.

Desde los atentados del 11 de Septiembre, el debate entre los límites de la privacidad y la seguridad ha estado abierto. Las filtraciones de Edward Snowden sobre el programa PRISM de espionaje a 35 líderes mundiales y las posteriores revelaciones sobre la

² "La recopilación y análisis de información en smartphones puede proporcionar sorprendentes conocimientos sobre cómo se mueven y comportan las personas", <http://goo.gl/5F4ODk>,

³ "Commission proposes a comprehensive reform of the data protection rules", Comisión Europea, <http://goo.gl/LlrTix>,

recopilación y vigilancia de datos por parte de la **Nacional Security Agency** de Estados Unidos, no han hecho nada más que reavivar el debate desde una perspectiva más gubernamental. Entre las noticias más destacadas sobre la invasión de la privacidad y el espionaje realizado por la NSA, se encuentran el acceso a los servidores de Google y Yahoo bajo el proyecto denominado MUSCULAR, con colaboración de la agencia británica *Government Communications Headquarters* (GGHQ), o que la NSA guarda 5.000 millones de registros al día sobre la ubicación de teléfonos móviles⁴.

Diversas compañías como **Microsoft, Google, Yahoo o Facebook**, han mostrado su preocupación y la intención de establecer **mecanismos que garanticen la privacidad** de sus comunicaciones. Microsoft por ejemplo está trabajando para proteger su infraestructura de comunicaciones entre sus centros de datos con un cifrado robusto que impida que sus datos puedan ser desvelados.

Como se puede deducir de lo anteriormente expuesto urge, por tanto, establecer mecanismos de protección y seguridad a los ciudadanos pero intentando salvaguardar su privacidad. Sin embargo, ambos son objetivos contrapuestos y es difícil establecer una frontera entre el derecho a la intimidad y el derecho a la seguridad.

2.1 Circunstancias Geopolíticas

En el panorama internacional, el análisis de la regulación y normalización en relación a la protección de datos y la privacidad debe tener en cuenta diversos factores, como los culturales, la regulación propia de cada país, y la relación entre economía y tecnología. Este último factor, el económico, es muy relevante, pues tal y como se ha ido desarrollando en este informe, y como se estudiará en la sección *Economía Basada en Datos* se ha desarrollado un completo modelo de negocio alrededor del tratamiento de la información personal.

Con respecto a la regulación interna de cada país, a mediados del año 2013, 99 países habían desarrollado o estaban desarrollando una legislación al efecto⁵. La Unión Europea ha establecido diversos acuerdos con países como Australia, Canadá, Argentina o Estados Unidos, además de estar adheridos al protocolo *Safe Harbour*⁶. Es, por tanto,

⁴ La NSA recopila 5.000 millones de datos al día sobre móviles", ABC, 5 de diciembre de 2013, <http://goo.gl/CCX40w>

⁵ Greenleaf, G "Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories", *Journal of Law, Information & Science*.

⁶ Commission decisions on the adequacy of the protection of personal data in third countries <http://goo.gl/88xvSu>

evidente que se están realizando esfuerzos en la **estandarización de los niveles normativos**. Estos esfuerzos han desembocado en la *Resolution on the Future of Privacy* de la 34 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad que ha decidido que sus miembros deben:

- 1.- **Intensificar la cooperación** entre ellos para responder a los riesgos transfronterizos en materia de protección de datos y privacidad de una forma coordinada, mediante la adhesión y refuerzo de redes de cooperación multilaterales.
- 2.- **Compartir la máxima información** y experiencia para asegurar la optimización del uso de los recursos escasos que disponen las autoridades.
- 3.- **Utilizar la oportunidad actual** para conseguir un mayor grado de interoperabilidad entre diversos sistemas legales y regímenes.

A nivel internacional, en el plano gubernamental, por ejemplo, la presidenta de Brasil, Dilma Rousseff, ha solicitado en noviembre de 2013 a la Organización de Naciones Unidas (ONU) que conceda prioridad a las discusiones sobre la privacidad en internet, y los gobiernos de Brasil y Alemania están impulsando un proyecto para frenar el espionaje electrónico, apoyado por la Vicepresidenta y Comisaria Europea de Justicia, Viviane Reding.

La resolución descrita anteriormente pide que los Estados miembros adopten medidas para poner fin a la violación del derecho de la privacidad en internet; aprueben legislaciones que garanticen el cumplimiento del derecho humanitario internacional y revisen sus actuales prácticas sobre la vigilancia de las comunicaciones y la recolección de datos personales.

En el marco de la Unión Europea y como reacción ante el caso de espionaje de la NSA, Viviane Reding ha propuesto la creación de un servicio de inteligencia europeo como contrapeso al NSA estadounidense. Como paso previo y como marco para la creación de esta futura agencia, se aprobará previsiblemente en los primeros meses de 2014 la nueva regulación de datos de la Unión Europea, que establecerá la frontera de la legalidad de lo que se puede hacer y no hacer en materia de protección de datos e Internet.

España ha estado ligeramente retrasada en la adopción de políticas y medidas que garanticen la ciberseguridad y la protección de datos, sin embargo es consciente de los peligros y las amenazas y está avanzando para solucionarlos.



Una respuesta clara a este problema es la Estrategia de Ciberseguridad Nacional, aprobada el 5 de diciembre de 2013 por el Consejo de Seguridad Nacional y que tiene su principio de funcionamiento en el Esquema Nacional de Seguridad del Real Decreto 3/2010 y en el Esquema Nacional de Seguridad de 2013. En este último, la Ciberseguridad se establece como una de los *riesgos o amenazas* para la Seguridad Nacional.

Ligado a lo anterior y con respecto al panorama tecno-económico internacional, podemos encontrar diferentes ejes en el mercado de las tecnologías de la información y las comunicaciones. La Figura 1, obtenida de la ITU (Unión Internacional de Telecomunicaciones), muestra las **20 principales economías** con respecto a los servicios de telecomunicación en 2010.

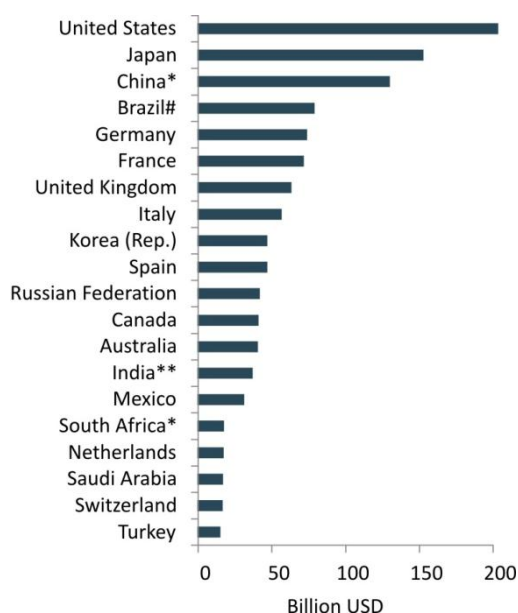


Figura 1: 20 mayores economías con respecto a los servicios de telecomunicación⁷

⁷ Measuring the Information Society 2012, International Telecommunications Union, 2012, <http://goo.gl/dPLHWW>

Analizando la tabla se pueden observar los ejes económicos clásicos. El formado por los países europeos, el de los países latinoamericanos, el conformado por EEUU, Japón y Canadá y el de los países asiáticos, como China y Corea.

Teniendo en mente estos dos factores y observando la distribución de la participación en la **Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, 2012**, que se muestra en la figura 2, se puede inferir que actualmente **Europa, Latinoamérica y EEUU están marcando la pauta** a seguir en cuanto al desarrollo internacional de los acuerdos en protección de datos y privacidad. Desde la perspectiva europea, el establecimiento de una posición de liderazgo con alianzas y acuerdos firmes en esta cuestión es muy relevante como contrapeso al eje asiático con el que las diferencias regulatorias y culturales son mucho más marcadas.

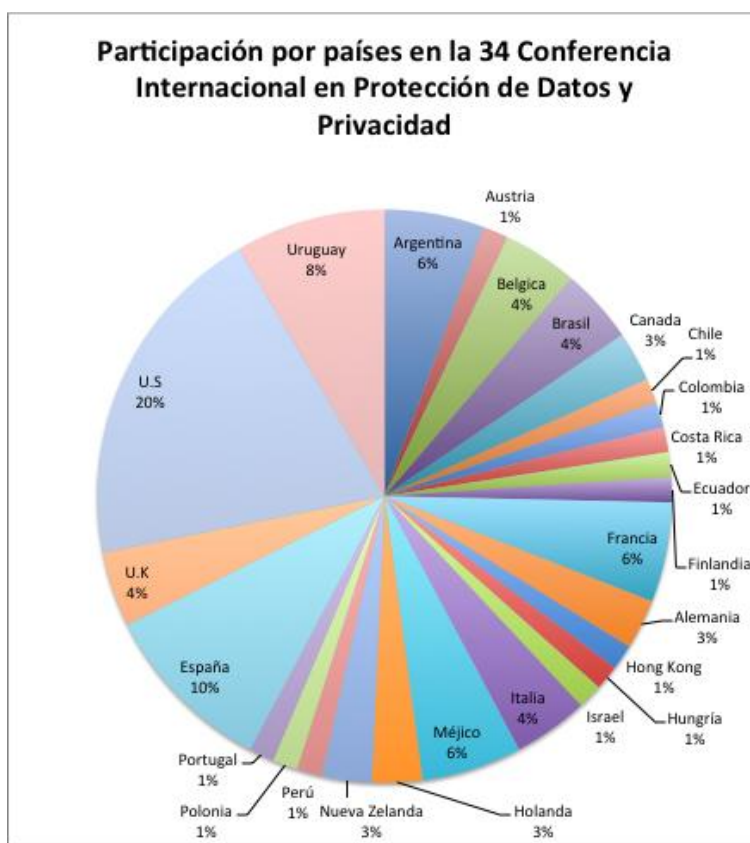


Figura 2: Distribución por países de la asistencia a la Conferencia Internacional de Protección de Datos, 2012, Fuente: elaboración propia.

3 PRIVACIDAD, PROTECCIÓN DE DATOS Y TENDENCIAS TIC

3.1 Redes Sociales: Responsabilidad Compartida

Las redes sociales (RRSS) han pasado a ser parte intrínseca de nuestra vida. Según el estudio de redes sociales realizado por IAB Spain, publicado en Enero de 2013, el 79 % de los Internautas españoles entre 18 y 55 años es usuario habitual de las mismas, accediendo a ellas, **en un 80 % de los casos, con periodicidad**



diaria, lo cual, evidentemente, ha llevado a incrementar, aun más, su importancia económica.

Una red social, se basa en facilitar a los usuarios la capacidad de compartir contenidos proporcionado por los mismos usuarios, para poder interactuar con otros usuarios registrados, dependiendo de los permisos establecidos en unos determinados perfiles de acceso⁸.

En la propia esencia de las RRSS se pueden llegar a intuir los primeros problemas relacionados con la privacidad, principalmente en aquellas redes de carácter generalista como Facebook o Twitter:

- **Existencia de un registro**, donde el usuario proporciona datos de carácter personal, de mayor o menor nivel de intimidad y que pueden ser accedidos por otros usuarios dependiendo del nivel de confidencialidad que se establezca.
- **Compartición de información** en múltiples formatos. Esta información puede contener datos personales o información privada, no solo del usuario, sino también de otras personas, usuarias o no de la red social. Un ejemplo claro de este caso es la publicación de fotografías de grupo en la red.
- **Interacción con usuarios** personales o profesionales: de la propia red de contactos, de la información publicada y de las preferencias de cada usuario se puede llegar a inferir perfiles de comportamiento.

⁸ Para la definición del término de Redes Sociales ver Anexo I

Sin embargo, la lista de peligros potenciales de las redes sociales en cuanto a la privacidad y protección de datos es claramente mayor. Existen casos de RRSS cuyas políticas de privacidad establecen que la red adquiere los derechos de todas las fotos que se suben a la misma, los contenidos, etc. (Facebook, Twitter...).

Otros peligros potenciales en las RRSS son las aplicaciones y juegos dentro de las propias redes, que, al instalarse, obtienen acceso a datos proporcionados por el usuario, datos relacionados con su perfil, sus contactos y en ocasiones a datos almacenados en el dispositivo desde el que se accede (smartphone, tableta....).

Por otra parte, en la mayoría de RRSS existe un **escaso o inexistente control sobre la veracidad de los datos** introducidos en el perfil. De esta manera se dan casos de RRSS orientadas a menores de edad donde pueden acceder personas mayores y RRSS orientadas a mayores de edad pero a las que acceden menores falseando los datos relativos a la edad, con el consiguiente peligro de ser objeto de acoso, abusos, y en definitiva, acceder a contenidos no orientados a menores.

Otro problema abierto son los mecanismos para **darse de baja**, así como para el ejercicio de los derechos de acceso, bloqueo y cancelación de los datos personales en las RRSS o la calidad y actualidad de los mismos. Los datos privados y personales sobre un determinado usuario publicados por otros usuarios, permanecen en la red social aun cuando éste se ha dado de baja, por lo tanto existe un problema en cuanto a la calidad y actualidad de los datos. Este **"derecho al olvido"** es un problema inherente a las redes sociales desde su expansión global. Ya en 2011, el por entonces responsable de privacidad en Europa de Facebook, Richard Allan, se mostró contrario a la intención de la Unión Europea de garantizar el derecho al olvido en Internet. Por otra parte en Junio de 2013, el abogado general del **Tribunal de Justicia de la UE** estableció un dictamen preliminar por el que la empresa **Google**, aún estando sujeta a la legislación de la UE sobre privacidad, **no está obligada a borrar la información** sensible de su índice de búsqueda, sino que el borrado debe realizarlo la fuente que lo publica.

Estas circunstancias hacen que la eliminación de datos personales y/o privados de un usuario en Internet en general, y en las RRSS en particular sea, a día de hoy, utópico, no existiendo, de hecho, el derecho al olvido. Esto perjudica claramente a los usuarios, tanto nativos digitales como los que no lo son, desde el punto de vista de su "Reputación Digital", pues inconscientemente pueden publicar información que les perjudique en el medio o largo plazo. Un estudio de *Young People's Consumer Confidence* (YPCC) que ha analizado a 6.000 jóvenes de entre 16 y 34 años en seis

países diferentes para evaluar el impacto de los medios en sus carreras como profesionales, ha concluido que uno de cada diez jóvenes ha sido rechazado para un trabajo debido a su perfil en las redes sociales.

Finalmente, no se deben obviar las cuestiones relacionadas con la ciberseguridad. Las RRSS y sus usuarios son objeto incremental de ciberataques. Existen diversos ejemplos recientes como el ocurrido en agosto de 2013, cuando el hacker Khalil Shreateh encontró una brecha de seguridad en Facebook que demostró en el muro de su propio creador, o la del 24 de Noviembre de 2013, cuando los investigadores de Trustwave's Spiderlab han descubierto más de 2 millones de contraseñas robadas de diversas redes sociales, entre ellas, 326.000 cuentas de Facebook, unas 60.000 de Google, más de 59.000 cuentas de Yahoo y cerca de 22.000 de Twitter. **Las técnicas de ciberataque** más típicas en RRSS son las siguientes:

- **Phishing y Robo de identidad:** Un ejemplo típico de uso en RRSS es la generación de eventos que son remitidos a los usuarios para confirmar su asistencia. Cuando se accede al enlace de la página de destino, se pide rellenar datos adicionales, entre ellos el nombre de usuario y contraseña.
- **Bots en RRSS:** Usuarios fantasmas que, a través de cuentas falsas, intentan conseguir un número muy alto de usuarios en poco tiempo con el objeto de intentar acceder a sus datos personales. En otras ocasiones proporcionan links que enlazan páginas de contenido malicioso para infectar la computadora del usuario.
- **Troyanos:** Por lo general, actúan invitando al usuario a descargar un archivo que le permite acceder a nuevas funcionalidades en la red social. La siguiente figura presenta un ejemplo para la red social Facebook.

Código malicioso (*malware*)



Figura 3: Ejemplo de troyano para la RRSS Facebook⁹.

- **Clickjacking:** Su definición formal es la práctica maliciosa que consiste en manipular la actividad de un usuario en un sitio web (típicamente una RRSS) camuflando enlaces por debajo del contenido legítimo “clickable” (como por ejemplo los “me gusta” de Facebook) o de botones de acción, produciendo acciones que el usuario desconoce. En muchos casos esto produce la compartición de los datos personales del usuario con el hacker desarrollador.

Además de estas prácticas, previamente existentes en el uso común de Internet, con el auge de las redes sociales han aparecido nuevas prácticas, que deben ser consideradas cuanto menos como infracciones. Una de las más extendidas es el ciberbullying, que en general se da sobre menores por parte de otros menores. Este no es un problema baladí, puesto que ya se han dado casos de personas que han cometido suicidio por no poder soportar la presión a la que están sometidos desde las redes sociales. La administración debe proporcionar instrumentos, seguramente fuera del ámbito policial¹⁰, para que los padres y responsables de los menores, o, con carácter general, para que

⁹ Imagen obtenida de la presentación del “Diagnóstico sobre la seguridad de la información y la privacidad en las redes sociales”, del Instituto Nacional de Tecnologías de la Comunicación INTECO, 2 de Julio de 2009.

¹⁰ Comparecencia de Eugenio Fontán Oñate, Decano-Presidente del Colegio Oficial de Ingenieros de Telecomunicación (COIT), ante la Ponencia conjunta de estudio sobre los riesgos derivados del uso de la Red por parte de los menores, Congreso de los Diputados 30 de enero de 2014

cualquier persona que sufra una de estas prácticas, tenga la seguridad de ser escuchado, atendido y de ver su problema resuelto.

Ante la anterior enumeración de peligros potenciales en las RRSS puede parecer que, tanto el mero registro como el posterior uso de las mismas, implica directamente una pérdida completa de la privacidad de los usuarios así como la exposición abierta a acciones delictivas por parte de terceros. En general esto no es completamente cierto, y si bien la utilización de las RRSS tiene muchas facetas positivas, en la sociedad actual es adecuado tener en cuenta las recomendaciones que proporcionan diversos organismos, como por ejemplo el INTECO y la AGPD¹¹, para salvaguardar la intimidad y la privacidad de los usuarios.



Las recomendaciones que realizan estas entidades se dirigen no sólo a los usuarios, sino también a las empresas del sector, para aumentar sus niveles de seguridad en las infraestructuras y mejorar la transparencia e información a los usuarios y a las administraciones públicas para mejorar la normativa aplicable y garantizar los derechos de los usuarios.

3.2 Cloud: Sistema y Almacenamiento en la nube

Uno de los términos más de moda en el panorama actual de las TIC es *Cloud* o *Cloud Computing*¹¹. En su modo más simple, el servicio *cloud* es simplemente de almacenamiento de datos, *Infrastructure as a Service (IaaS)*. Modelos más complejos pueden ser el *Software as a Service (SaaS)*, donde el usuario utiliza aplicaciones del proveedor mediante una sencilla aplicación cliente en su terminal y el *Platform as a Service (PaaS)*, donde el proveedor proporciona herramientas de desarrollo, como base de datos y aplicaciones, al cliente.



¹¹ Para una delimitación del término de Cloud y de sus tipos ver Anexo I

Aunque en general las empresas que proporcionan servicios *cloud* ofertan los tres modelos anteriormente señalados, a modo de ejemplo ilustrativo se ofrece la siguiente tabla¹².

Modo	Empresa
IaaS	DropBox. Rapidshare, Storage
SaaS	Google Drive (Google), Whitehat, Salesforce
PaaS	Google App Engine, Oracle, IBM CloudService

Es fácil entender que, desde el punto de vista de la privacidad y protección de datos, la provisión de **servicios cloud implica** que, en muchos casos, **la información privada** del usuario no se encuentra en la infraestructura física de su proveedor de servicios, sino que **está en la infraestructura de un tercero**, ya sea para su simple almacenamiento o para su tratamiento.

Para poder describir algunas de las diversas situaciones que ocurren en la provisión de servicios cloud, se proporciona el esquema de la Figura 4, que muestra las interacciones entre los participantes, así como los puntos más débiles, desde la perspectiva de la privacidad de los datos.

El cliente (usuario) que es el objeto final de la protección, puede contratar los servicios de *cloud* directamente, o tener contratado un servicio, no necesariamente TIC, con una determinada empresa, (1). Finalmente el proveedor de servicios *cloud* (2), puede tener su propia infraestructura para proporcionar los servicios o pueden ser subcontratados a otras compañía (3).

¹² "Top PaaS, SaaS and IaaS Cloud Companies by CloudTimes", www.cloudtimes.org

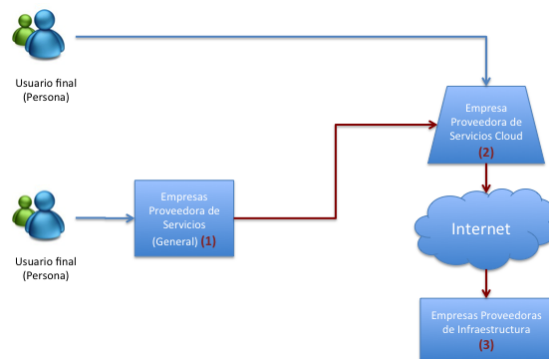


Figura 4: Esquema de interacciones en servicios cloud, Fuente:elaboración propia

Cuando la **contratación** de un determinado servicio la realiza un **usuario particular**, como por ejemplo el almacenamiento de información en un espacio virtual de DropBox, es la **empresa proveedora** de servicios *cloud* la que debe asegurar el nivel de protección adecuado para los datos personales de este usuario, pues es la empresa la **Responsable del Fichero**. No obstante, el usuario a la hora de contratar debe cerciorarse de las garantías que proporciona la empresa. Se debe tener en cuenta que en este caso la información de carácter personal se refiere únicamente a la de la persona física contratante, pues no existe, en este caso, un fichero de datos de carácter personal.

La situación cambia cuando la contratación del servicio *cloud* lo realiza una empresa/profesional para proporcionar unos determinados servicios a unos usuarios finales. En este caso la empresa (1) es la que tiene el papel de *Responsable del Fichero*, mientras que la empresa proveedora de servicios *cloud* (2) tiene el papel de *Encargado de Tratamiento*. Es la empresa (1) la que debe garantizar que tanto (2) como todas aquellas empresas de las que haga uso, cumplan los estándares de seguridad definidos por la Ley Orgánica de Protección de Datos y su correspondiente Reglamento, independientemente de si las empresas (2) y (3) se encuentran en España o fuera de España. En este último caso, en que o (2) y/o (3) estén fuera del territorio nacional, se considerará una transferencia internacional de datos y se debe garantizar los estándares de seguridad. Finalmente el proveedor de servicios (1) deberá garantizar la correcta ejecución de todos los derechos, tanto los de acceso, rectificación, cancelación y oposición, como la recuperación de datos y su portabilidad a otro proveedor cuando bien (2) o (3) dejen de ofrecer las garantías de seguridad suficientes.

En resumen, es el proveedor de servicios finales al usuario el que tiene la responsabilidad completa de garantizar la privacidad y protección de los datos de carácter personal de sus clientes.

3.3 Big Data: Máximo aprovechamiento de los datos

Otra de las tendencias importantes en el sector TIC actual, que se encuentra íntimamente relacionada con el *Cloud Computing* es el denominado *Big Data*¹³, que ha sido incluido por la consultora **Gartner** entre las **10 tendencias más importantes para el año 2013 y siguientes**.

Existen diversos ámbitos en los que se puede aplicar, y generar negocio con *Big Data*, (ver Figura 5), y mucha de la información que se recoge y utiliza, implica la utilización de datos de carácter personal.

Seguidamente mostramos algunos ejemplos de casos de negocio en los que se usan datos de carácter personal, centrándonos principalmente en *Retail/Marketing* y Banca/Aseguradoras por ser casos paradigmáticos.

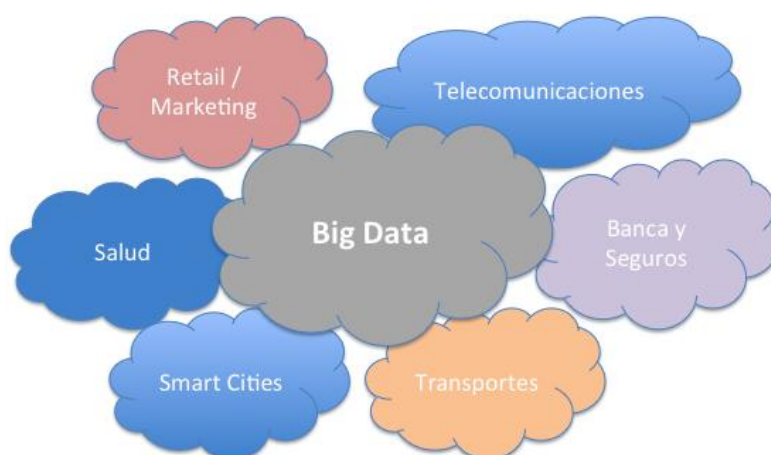


Figura 5: Campos de aplicación del Big Data. Fuente: elaboración propia.

- La compañía **Amazon** recoge información sobre el tipo de compras que se realizan, por ejemplo, tipo de libros, extensión, autores, tipo de accesorios (gadgets), etc, para ofrecer a cada usuario concreto nuevos productos adecuados a su perfil que le motiven a adquirirlos.
- Monitorización en tiempo real de los clientes de **American Apparel** (Cadena de Moda). Mediante reconocimiento facial se sigue el recorrido de las personas en una tienda y así se optimiza la distribución y tipología de productos.

¹³ Para una definición del término de Big Data, ver Anexo I

- Aplicaciones para smartphones: casi todas las grandes empresas disponen de un conjunto de aplicaciones para Smartphone, en la que proporcionan cupones para descuentos, servicios de localización de establecimientos, productos de fidelización, catálogos online e incluso juegos¹⁴. Con estos productos se recaba información del usuario para la creación de perfiles de marketing y diseñar campañas o promociones más adecuadas.
- Cálculo de costes/primas de seguros. Mediante dispositivos embarcados en el automóvil, empresas como **Detector** pueden obtener el comportamiento del usuario y así proporcionar datos a las aseguradoras para recalcular primas de riesgo¹⁵. Por otra parte en el cálculo de los seguros de vida, los datos de localización de la vivienda, compras, movimientos, viajes y vida laboral permitirán deducir el estilo de vida y utilizarlo en un modelo predictivo para los cálculos correspondientes¹⁶.

Existen varios factores a considerar dentro de la relación Big Data – Protección de Datos:

1. Recopilación de datos por parte de los usuarios

En relación con la privacidad, cada vez que un usuario pulsa un botón de “me gusta”, ya sea en Facebook, o un “reply” en cualquier otra aplicación, se están generando datos. En muchas ocasiones los usuarios aceptan unas condiciones de servicio para una tipología de datos determinada, como por ejemplo localización en la aplicación FourSquare. Sin embargo, el tratamiento conjunto de información obtenida por diferentes medios puede conducir a perfiles de usuario con ciertas características personales a las que no se ha dado permiso directo o indirecto.

2. Finalidad de los datos recogidos

En relación con la finalidad de los datos recogidos por sistemas o aplicaciones que puedan incorporarse a bases de Big Data se puede alegar que se aceptan las cláusulas de “*Términos y Condiciones*” que aparecen en la mayoría de ellas. Sin embargo al incorporarse al sistema de Big Data, se pueden obtener o abstraer

¹⁴ D. Avenick, D. Busk (The Coca Cola Company) and D. Pouliout (Google), “Consumer Engagement and Social Media Connecting With Digital Consumers Through Mobile And Social Platforms”, NAMA Oneshow, Abril 2012.

¹⁵ <http://goo.gl/XnG2dW>

¹⁶ L. Rossouw, “Big Data, Grandes Oportunidades”, Gen Re Jorunal, Junio 2012, vol 16, nº 2

perfiles que identifiquen comportamientos del usuario cuyo uso puede ir en contra de los propios intereses del usuario.

El principio de la limitación de la finalidad de la LOPD establece en su artículo 4.: *"Los datos de carácter personal, objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".*

3. Seguridad

El hecho de disponer de una cantidad masiva de datos de distintas personas implica obligatoriamente la existencia de grandes recursos informáticos que pueden ser motivo de ciberataques. Por otro lado, aunque los datos recogidos sean de nivel básico, al procesarlos, se crean perfiles que pasan a ser, como mínimo de nivel medio, llegando a ser incluso de nivel alto si se detectan usos médicos, políticos o religiosos.

4. Transparencia

El propio usuario seguramente desconozca la existencia de un perfil obtenido del procesamiento. Éticamente hablando, la empresa debería ser transparente con el usuario en cuanto a la existencia de ese perfil, de cómo se ha conseguido, y pidiendo la autorización del mismo.

5. Actualidad

El usuario tiene derecho a que sus datos sean actuales, y la empresa tiene la obligación de mantenerlos actualizados. Datos pasados pueden conducir a perfiles erróneos u obsoletos que perjudiquen los intereses del usuario.

El auge del Big Data así como sus posibilidades puede crear incertidumbres con respecto a la privacidad, la intimidad y la protección de datos. Estas incertidumbres, riesgos o problemáticas están íntimamente relacionadas con aquellas que se describieron en la sección de Redes Sociales, puesto que son estas una de las posibles fuentes de datos de las que se pueden alimentar algunos procesos de Big Data. En estos casos, las recomendaciones para los usuarios son las ya indicadas.

En otras ocasiones, los datos procesados por empresas relacionadas con el *Big Data* son directamente recopilados de los usuarios por estas, por ejemplo, en el momento de contratación de un determinado servicio (seguro, cuenta bancaria) o al registrarse e interactuar en un sitio de compras online. En este caso, el usuario debe ser consciente que todos sus datos, están cubiertos por la normativa de protección de datos, y que por

lo tanto puede ejercer sus derechos de acceso, rectificación, cancelación y oposición contra la empresa. Por otra parte, en caso de que, a través de los datos proporcionados se puedan generar perfiles de uso, éstos deben tener una finalidad acorde con el propósito con el que han sido recabados y el usuario tendrá derecho a estar informado de los mismos y a oponerse en caso de que se utilicen para otras finalidades. Finalmente, en caso de que el resultado del procesamiento de estos datos sea cedido a otra empresa, el usuario debe dar su consentimiento explícito para ello.

Big Data es una tendencia muy importante que puede generar nuevos e importantes modelos de negocio, tal y como se mostrará en la sección *Economía Basada en Datos*, pero la generación de estos nuevos negocios no debe ir en detrimento de la privacidad de los usuarios.

3.4 El problema de los Call Centers

Una de las que probablemente, desde el punto de vista del usuario final, sea una de las invasiones más flagrantes de la privacidad de los usuarios que ha surgido en la última década, es la de las llamadas de los *Call – Centers*. Estos centros han sido utilizados por todo tipo de empresas, entre ellas las telecomunicaciones, eléctricas, gasísticas y aseguradoras principalmente, para muy diversos fines, entre ellos la promoción activa de sus nuevos productos y la captación de nuevos clientes.

El método de operación más común es que los datos de los usuarios se añaden a un fichero de datos de carácter personal “*que podrá ser utilizado para fines publicitarios, marketing y otros diversos relacionados con la compañía del grupo...*” en el momento de la contratación.



Usualmente estas compañías no son, denominémoslas, individuales, sino que pertenecen a grupos mayores, en ocasiones multinacionales, con multitud de filiales que se dedican a diversos negocios. Por lo tanto en el momento de la aceptación del contrato, los datos del usuario pueden ser utilizados para fines promocionales por cualquiera de las filiales del grupo.

Existen por supuesto medios para evitar el intrusismo de los *call center*, tanto directos, como el ejercicio de derechos de oposición y cancelación, como indirectos, como la inclusión del usuario en las Lista Robinson¹⁷.

Sin embargo el panorama actual es más complejo. En muchas ocasiones debido a la deslocalización, las empresas de *call-center* se encuentran fuera de España, en países confiables o en empresas que han firmado el protocolo Safe Harbour¹⁸. En su mayoría, las empresas de *call center* con las que se firma un contrato de tratamiento de datos que implique una transferencia internacional, ya requiera aprobación o no del Director de la APD, son empresas confiables. Sin embargo siempre existen excepciones, que pueden llegar a comercializar los datos. La Figura 7 presenta un posible esquema donde en verde se muestran las transacciones legales y en rojo las ilegales.

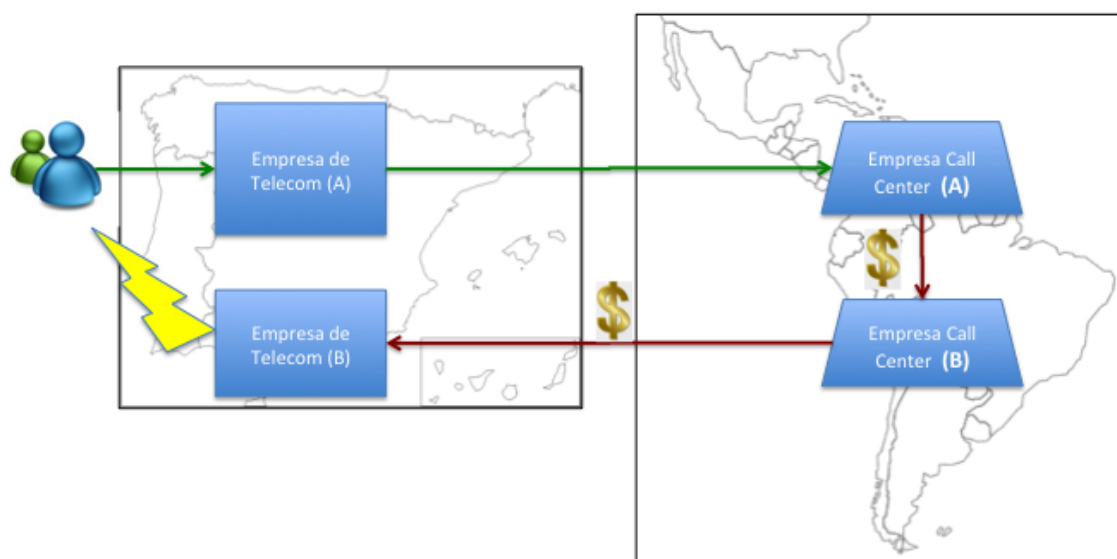


Figura 7: Esquema de transacciones internacionales de datos en Call Centers. Fuente: elaboración propia.

Parece obvio que las empresas (B) y el *call center* (A) son claramente sancionables y así lo estipula la AGPD. El propio hecho de la adquisición de datos del *call center* (B) por la empresa (B) es irregular, pues al ser datos de carácter personal debe tener el permiso expreso de los usuarios finales. Además, aunque la empresa (A) haya realizado todas las gestiones de manera correcta y sea el *call center* (A) el que

¹⁷ Listas Robinson www.listarobinson.es

¹⁸ Agencia de Protección de Datos, Listado de países con transferencia internacional de datos. <http://goo.gl/5IXUG>

comienza las infracciones con respecto a los datos, la propia empresa (A), al ser el *Responsable del Fichero* es el responsable último de las medidas de seguridad y transparencia del call center (A), que es su *Encargado de Tratamiento*.

Aunque el marco regulatorio para la cesión y tratamiento de datos, ya sea con carácter nacional o internacional, esté claramente estipulado, lo cierto es que las transferencias no autorizadas nacionales e internacionales de datos se están realizando. En el año 2012 la AGPD impuso sanciones por un montante de 21 millones de euros por incumplimiento de la ley. El 73 % de estas sanciones fueron a empresas de telecomunicaciones¹⁹. El propio director de la agencia, D. Jesús Rubí ha indicado que los países latinoamericanos son los principales importadores de datos de España y que en esta transferencia internacional de datos tienen una participación muy importante los denominados Call Center. Esto implica que, a día de hoy el negocio de las transacciones de datos es suficientemente lucrativo para arriesgarse a las sanciones.

4 EL FUTURO DE LA REGULACIÓN ~2016

Como ya ha sido explicado a lo largo del informe, la creciente globalización de los flujos de datos, vía redes sociales, procesamiento en la nube, motores de búsqueda, servicios de localización, etc, incrementa el riesgo de que la gente pierda el control sobre sus propios datos.

El 21 de octubre de 2013, el Parlamento Europeo se inclinó a favor de realizar una revisión del reglamento europeo de protección de datos con el objeto expreso de retornar el control a la población de sus datos personales, fomentar la confianza en las redes sociales y en las compras online, y mejorar la protección de los datos procesados por la policía y las autoridades judiciales.



¹⁹ “España aplicó multas por 21 millones de euros por incumplir protección datos”, El País, 11 de Septiembre de 2013, <http://goo.gl/TRi2FY>

La nueva ley reemplaza el actual rompecabezas de leyes nacionales con un único conjunto de leyes que debe facilitar a las compañías su movilidad en la UE, a la vez que se protegen los derechos de los ciudadanos.

Las actuales leyes europeas de protección de datos datan de 1995, antes incluso de que Internet tuviera un uso masivo. A día de hoy, 250 millones de europeos usan Internet diariamente. Entre las carencias más significativas de la actual legislación se encuentra el limbo jurídico de los datos relacionados recabados para el cumplimiento de la ley y las intervenciones telefónicas por parte de los cuerpos y fuerzas de seguridad de los Estados.

El paquete de reformas propuesto consiste en dos borradores legislativos:

1. Un Reglamento General que cubre el grueso del procesamiento de datos en la UE.
2. Una Directiva en procesamiento de datos para prevenir, investigar, detectar o perseguir ofensas criminales o hacer cumplir penas criminales, protegiendo los datos de los ciudadanos.

El borrador del reglamento actualiza los principios establecidos en la directiva de 1995 para adaptarse a la nueva realidad de Internet incluyendo datos procesados de forma online: redes sociales, compras online y banca online; y offline: datos guardados en registros de universidades, hospitales y compañías.

Seguidamente se presentan algunos ejemplos de las propuestas presentadas por la Comisión:

- **Transferencias de datos fuera de la Unión Europea** (Artículo 43a): Las solicitudes de datos procesados dentro de la Unión Europea a compañías privadas (motor de búsqueda, red social o proveedor de datos en la nube) por parte de entidades gubernamentales de países ajenos a esta, deberán recabar el permiso de la autoridad nacional de protección de datos e informar a la persona afectada antes de realizar la transferencia de los mismos.
- **Sanciones para las compañías** (Artículo 79): Las autoridades de protección de datos impondrán al menos alguna de estas sanciones por los incumplimientos del reglamento:
 - Una advertencia por escrito, ante incumplimientos menores.
 - Una auditoría periódica en protección de datos.

- Para compañías privadas, una multa de hasta €100 millones o un 5% de su facturación.

Esta última propuesta es una de las más controvertidas ya que algunas firmas evalúan la opción de seguir incumpliendo el reglamento y abonar las correspondientes sanciones en lugar de modificar su operativa.

- **El derecho al borrado:** Cubre el “derecho al olvido” propuesto por la Comisión. Los ciudadanos podrán solicitar no sólo el borrado de sus datos personales, sino también el borrado de las réplicas de sus datos.
- Otros puntos cubiertos en el borrador son el consentimiento explícito (Artículo 7), el derecho a la información en un lenguaje claro y sencillo (artículo 11), los límites al uso de datos para crear perfiles, facilitar la portabilidad de datos para fomentar la competencia (Artículo 18), la asignación de un agente para la protección de datos en instituciones y empresas (Artículo 35), el derecho a quejarse sobre infracciones relacionadas con la protección de datos (Artículo 54), etc.

El borrador de la Directiva (el relacionado con las intervenciones y escuchas policiales) reemplaza a la decisión marco de 2008 sobre procesamiento de datos en cooperación policial y judicial. Está diseñado para proteger tanto los datos nacionales como las transferencias internacionales de datos, por ejemplo, restringiendo el almacenamiento y la transferencia de datos personales. En este sentido el profesor del MIT Alex Pentland, y asesor del World Economic Forum en esta materia, afirman que *“para lograr una sociedad justa en la era de los datos, debemos alcanzar un Nuevo Acuerdo sobre Datos, cuya clave es tratar los datos personales como un activo, sobre el que los individuos tienen derecho de propiedad”*. La propuesta de Pentland se basa en tres pilares: (1) derecho a la posesión de los datos, de manera independiente de qué entidad los recopile, (2) derecho al pleno control sobre los datos y (3) derecho a la disposición de los datos y su distribución. Es evidente que la situación actual no satisface estos principios aunque la nueva regulación europea está caminando en esta dirección.

Esta propuesta de la Comisión Europea está siendo tratada actualmente por el Consejo y el Parlamento Europeos, por ser un procedimiento de co-decisión. Las objeciones de algunos estados miembros, como Reino Unido, que prefieren una mayor autorregulación por parte de las compañías, y **las próximas elecciones al Parlamento pueden retrasar la aprobación** de la propuesta legislativa hasta mediados del 2015.

5 ECONOMÍA BASADA EN DATOS

Desde un punto de vista empresarial, los datos masivos (Big Data), entre ellos los datos personales, alteran la naturaleza de los negocios, y los mercados. A día de hoy los datos, ya no son un apoyo de las transacciones, sino que, en muchas ocasiones se convierten en el propio objeto del intercambio, como muestra un estudio de la OCDE "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value"²⁰

El valor de **los datos** de carácter personal no debe ser visto únicamente desde el punto de vista monetario, puesto que parte del mismo **tiene un carácter socio-económico**, por ejemplo, el uso de información personal para ahorrar en el número de pruebas médicas a realizar a los ciudadanos o para fomentar y promocionar la investigación en nuevos fármacos.

En la denominada cadena de valor de los datos intervienen numerosos actores como empresas privadas o instituciones públicas, siendo su participación en la misma global o parcial al estar implicados únicamente en algunos eslabones como se puede observar a continuación.

Cada tipo de datos de carácter personal, obtenido de forma voluntaria, observado o inferido, es inicialmente recogido o accedido, a continuación, almacenado y agregada para pasar a su procesamiento siendo finalmente utilizado como se observa en la figura 8.

²⁰ OECD (2013), "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", *OECD Digital Economy Papers*, No. 220, OECD Publishing.
doi: <http://goo.gl/PYlj12>

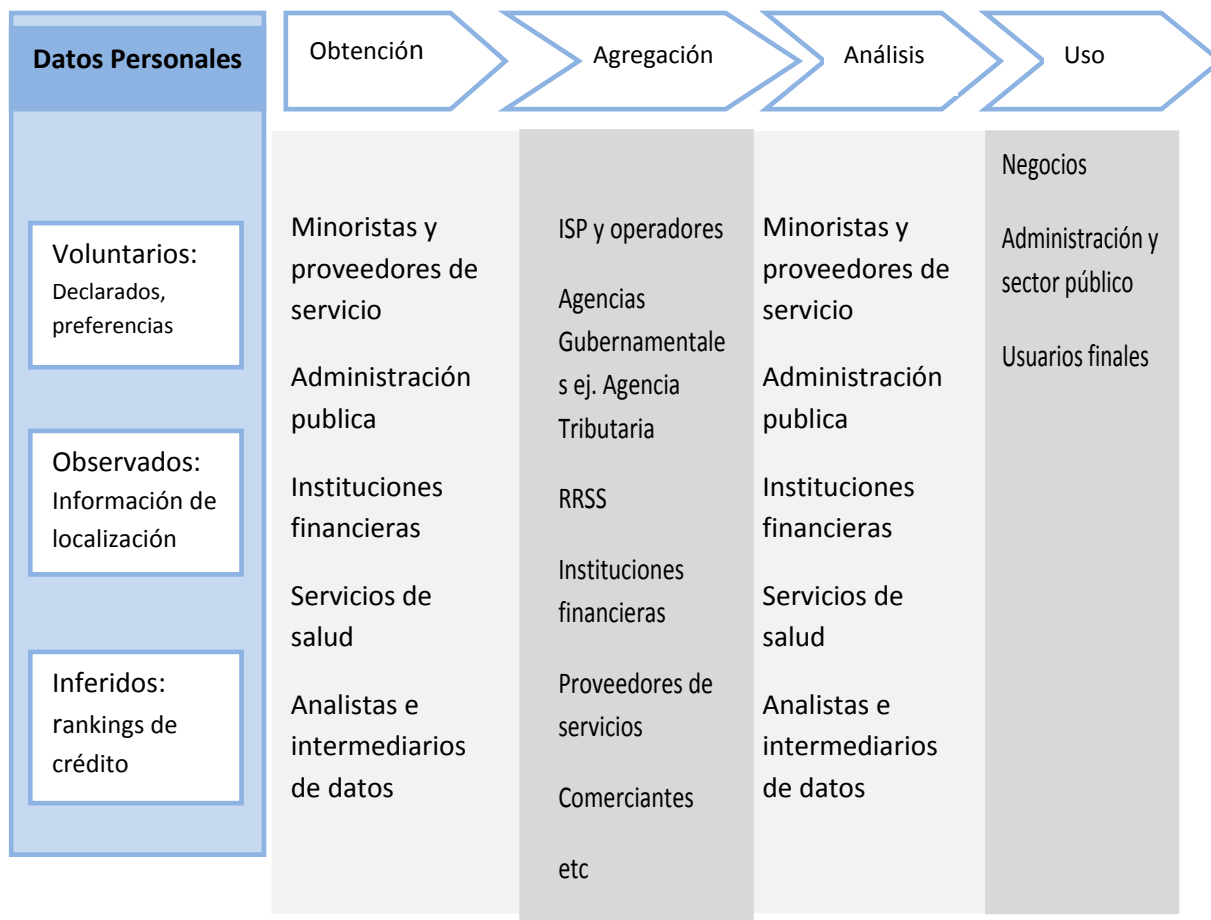


Figura 8: Cadena de valor de la economía basada en datos. Fuente OCDE.

Obtención de los datos personales: Este proceso abarca todos los sectores de la economía recogiendo los datos de una gran variedad de fuentes, tanto de forma directa como indirecta, por ej.: tarjetas de fidelización o el envío por parte de apps. Este paso es el que ha experimentado una mayor transformación debido al crecimiento del uso de las TIC en la sociedad.

Almacenamiento y agregación: los elementos individuales (datos) se organizan y se almacenan en conjuntos que se pueden utilizar para su posterior procesamiento y análisis. Actualmente el coste de almacenamiento no es apreciable y los problemas de acceso han desaparecido. Esto ha llevado a que este eslabón de la cadena pueda ser implementado por multitud de actores, por ej.: buscadores de internet, historiales médicos por hospitales, direcciones de empleados por las empresas.

Procesamiento, análisis y distribución: los datos almacenados deben ser combinados con otro tipo de información para desarrollar perfiles detallados. Esa

combinación incrementa su valor puesto que permite inferir información que no puede ser encontrada de otra manera.

Este eslabón es un punto clave en la cadena de valor. Aunque, desde el punto de vista tecnológico cualquier empresa familiarizada con CRM pudiera desarrollarlo, esta parte está siendo ocupada por empresas con una infraestructura desarrollada y gran capacidad de análisis. Un ejemplo son las empresas especializadas en publicidad on-line.

Utilización: una vez que los datos han sido recogidos, almacenados y analizados, a menudo se ponen a disposición de los usuarios finales en los mercados, lo que representa el final de la cadena de valor. Los usuarios suelen comprar los perfiles de las personas (o empresas) con el fin de complementar sus propias actividades empresariales.

Los datos personales se utilizan normalmente para mejorar el servicio a los clientes permitiendo implementar modelos de negocio centrados en el usuario. Los datos personales también se agregan para mejorar la eficiencia de las transacciones y operaciones comerciales, así como para identificar las tendencias macro en diferentes sectores, como el sanitario, logístico y el de seguridad.

Los datos personales aplicados al comercio en su sentido amplio permiten a las empresas realizar **modelos de negocio centrados en el usuario**, que aumentan la fidelidad de los clientes, debido a mejores experiencias de producto, y la personalización de las campañas de marketing. Un ejemplo de la mejora en la experiencia del cliente utilizando los datos de usuario es el ejecutado por la empresa Amazon. Su último desarrollo patentado consiste en un mecanismo²¹ para realizar el envío de los paquetes de compra al usuario antes de haber ejecutado el propio acto de compra, mejorando así el tiempo entre la solicitud y la entrega. Para ello se aprovecha del historial de compra, la lista de deseo de compras o la localización del usuario entre otras informaciones.

En la línea de obtener nuevos clientes con ofertas personalizadas, Apple ha presentado recientemente iBeacon²² integrado en su nuevo sistema operativo iOS 7. Éste determina la geolocalización exacta del usuario en interiores basándose en tecnología *bluetooth*. Mediante la localización exacta del cliente dentro de la tienda puede enviar mensajes,

²¹ Patente Amazon Tech Inc, "Method and system for anticipatory package shipping" "<http://goo.gl/uS22Nf>

²² D. Addey, "iBeacons", <http://daveaddey.com/?p=1252> y <http://goo.gl/kTr8q6>

ofertas o datos que se estima que pueden ser del interés del usuario, por ejemplo, si el cliente está delante de un iPad y dispone de un iPhone, el sistema envía ofertas promocionales sobre el iPad o sus accesorios.

Sin embargo, muchas compañías no poseen los datos para poder desarrollar este tipo de estrategias. Aquí surgen diversas empresas focalizadas en obtención de los datos personales, su almacenamiento y agregación. Estas empresas suelen recolectar los datos a través de aplicaciones móviles gratuitas o sistemas basados en conexiones de datos, por ejemplo *Wi-Fi*²³. Al aceptar el contrato de uso, se acepta la cesión de los datos personales, localización, acceso a la agenda del smartphone y un largo etc. En este caso la aplicación resulta ser solo un medio para obtener **el auténtico producto: los datos del usuario**, de manera que éste acaba convirtiéndose en el autentico producto. Adicionalmente existen empresas que, por su propia naturaleza, poseen una gran cantidad de datos y los licencian a terceros con el fin de maximizar el valor de los mismos. Un ejemplo es la empresa ITA Software, una gran red de reserva de vuelos.

Todos estos datos, junto con otros disponibles de forma pública, son agregados y cedidos a terceros para desarrollar servicios como los expuestos en los ejemplos anteriores. Este tipo de empresas, actualmente están presentando un gran crecimiento como Turnstyle, Viasense o Euclid Analytics, entre muchas otras.

Esta utilización de los datos ha permitido entrar en la denominada era smart: *smart grid, smart cities, smartphone, smart transport*,... donde los dispositivos ofrecen servicios utilizando esa inteligencia volviéndose más dinámicos, proactivos y por consiguiente, más adaptados al usuario, o incluso se adelantan a los propios deseos del mismo. Este tipo de paradigma entre sus principales elementos para poder desarrollarse es la capacidad de conocer los datos, a veces personales, del usuario. Por lo tanto para el desarrollo y el avance de este paradigma se desarrollan aplicaciones de captura de datos para poder ofrecer un mejor servicio al usuario.

Sin embargo, la economía basada en datos no está exenta de inconvenientes. El primero es que los usuarios, que tienen la sensación de acceder al contenido de forma gratuita, están pagando el servicio mediante la cesión de sus datos personales. Sin ninguna intención conceden un permiso "al por mayor", perdiendo la noción misma del consentimiento informado de la finalidad de los datos. Esto se debe a que la mayor

²³ A. G. Luna "El trato de las grandes marcas: tu intimidad a cambio de wifi gratis", El confidencial, 10 de Enero de 2014
<http://goo.gl/LQFNOC>

valorización de los datos se produce cuando estos son agregados²⁴. Además no hay que olvidar que los datos tienen una propiedad muy interesante: el valor de los mismos no disminuye cuando estos se usan; pueden volver a procesarse una y otra vez.

Actualmente muchas empresas están recolectando datos sin un propósito definido, porque entienden que el valor es almacenar los datos para uso futuro.

6 CONCLUSIONES

Actualmente, puede existir entre la población una sensación de cierta inseguridad ante posibles “mala-praxis” en relación a la utilización de datos de carácter personal e información privada. Esta sensación viene motivada porque el desarrollo de la tecnología ha facilitado la capacidad de recolección, almacenamiento y agregación de los datos y por el incremento de contenido en el mundo virtual de internet, ya sea a través de las redes sociales o de los servicios *cloud* entre otros. También contribuye en cierta manera la tendencia en los medios de comunicación, en mayor medida desde los sucesos de las filtraciones de Edward Snowden sobre la NSA, hacia los eventos relacionados con la privacidad y la protección de datos.

Sin embargo, esta misma revolución en el tratamiento de los datos ha permitido mejorar y hacer más eficientes los sistemas de salud mediante técnicas de predicción de enfermedades o estudios epidemiológicos, generar nuevos modelos de negocio que reactiven la economía u optimizar rutas logísticas y de desplazamiento de personas, mejorar los servicios ciudadanos. En definitiva, el tratamiento de los datos en general y de los datos personales en particular tiene facetas positivas y negativas que hay que balancear para encontrar un equilibrio que beneficie a los ciudadanos.

En este documento se ha procurado proporcionar una visión general de las implicaciones del manejo de datos en las tendencias actuales del sector TIC, siempre bajo una perspectiva de la protección y privacidad del usuario. Seguidamente se detallan algunas de las conclusiones principales.

Lo que está en Internet deja de ser privado

Internet en general y las redes sociales en particular son grandes acumuladores de información privada de difícil gestión en cuanto a su actualidad, finalidad y que además

²⁴ V. Mayer-Schönberger et al “Big Data: La revolución de los datos masivos”.

es prácticamente imposible de eliminar, por lo tanto, si el usuario no desea ver comprometida alguna información privada, no debe ser expuesta en la red.

Cedemos privacidad para mejorar los servicios.....

De la misma manera que se cede privacidad y comodidad para aumentar la seguridad, como por ejemplo en los servicios de transporte aéreo de personas, el usuario está cediendo parte de su privacidad, en ocasiones a través de los datos personales, para la mejora de servicios, ya sean ofrecidos por una empresa o por la propia administración.

.... pero se debe fomentar un adecuado desarrollo regulatorio...

La Directiva europea de protección de datos (95/46/CE) data del año 1995, la Ley Orgánica de Protección de Datos de Carácter Personal es del año 1999. Desde aquel entonces tanto la tecnología, los servicios, como la propia sociedad han cambiado, por lo que la regulación debe actualizarse para ofrecer un marco jurídico que responda a la situación actual.

....y se está trabajando en ello....

Actualmente se está produciendo un incremento de la normativa y regulación en el sector, especialmente en el año 2013, y se espera que se incremente con la aprobación de la nueva normativa Europea esperada a partir del 2014 o 2015.

...y Europa debe estar (y está) a la cabeza.

Europa se está poniendo al frente de la regulación, por la gran importancia que se le otorga a la privacidad, y se observa en las iniciativas y la adhesión a las distintas propuestas internacionales. Además, debido a que el concepto de privacidad es distinto dependiendo de la parte del mundo (Europa, Asia Oriental, Latinoamérica, Norteamérica e influencia anglosajona) es fundamental que el regulador europeo se coordine con aquellos países cuya herencia cultural sea más cercana a la europea, antes de que los ejes económicos fueren a otras componendas.

Los Datos, y no sólo los personales... son una fuente de crecimiento económico...

Se puede ver que la cadena de valor de los datos va más allá de los datos de carácter personal, puesto que se están recopilando datos de tipo no lingüísticos como el historial de navegación o aquellos basados en las emociones o tendencias para desarrollar innovadores modelos de negocio. De esta manera se está huyendo de los modelos más

tradicionales, y menos éticos, como es la venta de datos personales, por ejemplo, a compañías de tele-marketing o call centers.

...que se deben tratar conforme a buenas prácticas....

Este nuevo sector debe generar y adoptar buenas prácticas y recomendaciones que produzcan un incremento de la sensación de seguridad y confianza de los usuarios. Esto redundará en un mayor volumen de negocio, y evidentemente en un menor número de reclamaciones. La regulación también tiene que ir en este sentido, promoviendo el uso ético y adecuado de los datos y sancionando, como se sugiere actualmente para el Internet de las Cosas²⁵, con contundencia, las correspondientes acciones punibles.

²⁵ Estudio que destaca las carencias regulatorias ante esta explosión tecnológica. <http://goo.gl/kOlw2J>

7 ANEXO I

1 Cloud Computing

Según el National Institute of Standards and Technology (NIST) del U.S Commerce Departament, es un modelo para posibilitar un acceso adecuado, ubicuo y bajo demanda a un conjunto de recursos computacionales (servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y proporcionados al cliente, minimizando los esfuerzos de gestión y de interacción con el proveedor del servicio.

Lo que subyace de esta definición es que el usuario, sea este una persona física o jurídica, no dispone de una infraestructura de IT, sino que confía parcialmente o plenamente a un proveedor de servicios.

2 Redes Sociales

Según la consultora Gartner y el INTECO, una red social se puede definir como una plataforma online o sitio web donde los usuarios registrados con un determinado perfil personal o profesional comparten información, en cualquier formato, y pueden interactuar con otros usuarios registrados, dependiendo de unos determinados perfiles de acceso. Las redes más habituales en España son: Facebook, Twitter, Tuenti, Linkedin, Google+, Myspace, Youtube e Instagram entre otras.

3 Big Data

Existen diversas definiciones y concepciones de Big Data, una de las más adecuadas es la que proporciona la consultora Gartner, que indica que son “grandes volúmenes de registros de información variada que se generan a alta velocidad y que requieren de innovadoras y efectivas formas de procesado para proporcionar un mejor conocimiento en las tareas de apoyo a la decisión²⁶”.

²⁶ Traducción del autor







colegio oficial
ingenieros
de telecomunicación

Almagro, 2 28010
Madrid

Tel.: 91 391 10 66
Fax: 91 319 97 04
e-mail: coit@coit.es
web: www.coit.es