La información personal que se mueve en Internet no deja de crecer. Cada día, millones de personas utilizan servicios como redes sociales, foros, páginas de compra..., lo que deja un rastro de su actividad, gustos y preferencias, en definitiva de su comportamiento y forma de ser. Toda esta información amplía el concepto tradicional de identidad y lo lleva a una nueva dimensión. Ya no se trata de una identidad definida por rasgos físicos, ni por documentos que acreditan al portador unas capacidades y le habilitan para realizar ciertas actividades, sino de un concepto más amplio en el que la vida digital enriquece la vida real dando lugar a la Identidad Digital.

Como todo cambio importante, su introducción lleva implícito el desafío de aprovechar los beneficios que puedan obtenerse y a la vez tratar de esquivar los problemas que puedan generarse de su implantación. En el ámbito de la Identidad Digital, el equilibrio entre amenazas y oportunidades es un aspecto central que se aborda en este informe, ya que se pueden encontrar aspectos tanto en un sentido como en el otro. Y es que a veces no es fácil aprovechar los grandes beneficios que pueden obtenerse de una gestión adecuada de la Identidad Digital sin cruzar la línea que separa nuestra identidad de nuestra privacidad.

Este monográfico aborda el tema de la Identidad Digital de una forma objetiva y considerando diferentes puntos de vista. Se ha tenido un especial interés en mostrar las implicaciones que pueden tener en este ámbito diferentes líneas tecnológicas, como la seguridad, la nube, el *big data*..., por lo cual se incluyen gran cantidad de ejemplos de empresas innovadoras que utilizan estas tecnologías para ofrecer servicios relacionados con la Identidad Digital.

Al igual que sucede en los anteriores informes, el carácter amplio del tema tratado obliga a seguir un enfoque multidisciplinar. Por este motivo, se ha realizado un encuentro de expertos relevantes con diferentes perfiles que son necesarios tener en cuenta para ofrecer una visión global sobre el tema, cuya transcripción se incluye en el último capítulo del monográfico.

Fundación Telefónica

Identidad Digital: El nuevo usuario en el mundo digital

Ariel

Fundación Telefónica

Telefónica

Informe 23

Fundación Telefónica

Telefónica

Fundación Telefónica

Esta obra ha sido editada por Ariel y Fundación Telefónica, en colaboración con Editorial Planeta, que no comparten necesariamente los contenidos expresados en ella. Dichos contenidos son responsabilidad exclusiva de sus autores.

Coordinación editorial de Fundación Telefónica: Rosa María Sáinz Peña
Con la colaboración técnica de Telefónica I+D

Primera edición: Julio 2013

ISBN: 978-84-08-12110-7

Depósito legal: B. 18.329-2013
Impresión y encuadernación: Unigraf, S.L.

Impreso en España – Printed in Spain

El papel utilizado para la impresión de este libro es cien por cien libre de cloro y está calificado como **papel ecológico**.

Identidad Digital:
El nuevo usuario en el mundo digital

Ariel

Colección
Fundación Telefónica

Introducción general

La **identidad humana** puede definirse como el **conjunto de rasgos** que hace a una persona ser quien es y lo distingue de los otros al mismo tiempo que le permite interactuar en su entorno. Se construye en función de las condiciones de la propia persona pero también en función de los acontecimientos y las experiencias vividas, de hecho, la identidad humana **solo se realiza plenamente en función de la interacción con el medio externo** y se trata de una realidad que evoluciona a lo largo del tiempo. Adicionalmente, la necesidad de **un sentimiento de identidad es vital** e imperativa para el hombre.

En la actualidad, las nuevas tecnologías relacionadas con la información y las comunicaciones están ampliando el concepto de identidad complementándolo con el de **identidad digital**. Entre los datos que ayudan a configurar este nuevo concepto se encuentran los de identidad individual, los de comportamiento, los derivados o calculados por terceros y los que el propio usuario va creando para identificarse en el mundo digital. Como puede apreciarse, la construcción de esta identidad digital distingue entre la información que se revela expresamente por la persona, la identidad que es revelada por las acciones que esta realiza y la que es calculada o inferida según el análisis de las acciones que la persona lleva a cabo. En principio, no es nada nuevo respecto a la realidad que se da en el mundo físico. La diferencia está en **el potencial que le otorga a todo ello la tecnología**: la persistencia de la información, la trazabilidad y la ordenación cronológica y en que **el propio uso de la tecnología también incide en el propio comportamiento humano**, en cómo nos socializamos, en nuestra capacidad de concentración y en cómo gestionamos nuestra privacidad.

En este nuevo entorno, **identidad digital, información, privacidad y seguridad son aspectos que van muy unidos**, pues para poder gestionar correctamente la primera hay que poder gestionar los otros tres aspectos. Es razonable que la gestión de la privacidad sea el principal motor en la gestión de la identidad digital. En este ámbito el concepto de «propiedad sobre los datos» está evolucionando hacia el de «derecho sobre los datos» y en eso es, precisamente, en lo que inciden los sistemas que se dedican a gestionar la identidad digital.

No cabe duda del **gran valor de llevar a cabo una correcta gestión de la identidad digital**, tanto para la propia persona como para las diferentes empresas y organizaciones con las que esta interactúa, porque, sin lugar a dudas, **la persona tendrá que desenvolverse cada vez más en un mundo digital interconectado**.

Índice

«Who steals my purse steals trash... But he that filches from me my good name, robs me of that which not enriches him, and makes me poor indeed.»

William Shakespeare

Capítulo 1

¿Qué es lo que identifica a una persona?

El concepto de identidad humana puede definirse como el conjunto de rasgos que hace a una persona ser quien es y lo distingue de los otros, al mismo tiempo que le permite interactuar con su entorno.

La formación de la identidad es un proceso que comienza a configurarse a partir de ciertas condiciones propias de la persona, presentes desde el momento de su nacimiento y, a partir de ahí, evoluciona según los hechos y las experiencias que le acontecen a lo largo de su vida. La identidad humana se configura así a partir de la interacción con el medio y el funcionamiento individual propio del sujeto, formándose entre ellos una tensión dinámica que guía la configuración de la identidad hacia una dirección determinada.

La identidad humana puede definirse como el conjunto de rasgos que hace a una persona ser quien es y lo distingue de los otros al mismo tiempo que le permite interactuar con su entorno.

La identidad es, pues, un núcleo plástico capaz de modificarse a lo largo de la vida y se desarrolla en función de la interacción con el medio externo, ya que en una situación de aislamiento, las características individuales resultan irrelevantes. Así, es precisamente en relación con la interacción con los otros cuando las diferencias y las características individuales adquieren valor y se comportan como aportes para la interacción social.

Desde la perspectiva de la filosofía, según Erich Fromm, la necesidad de un sentimiento de identidad es tan vital e imperativa que el hombre no podría estar sano si no encontrara algún modo de satisfacerla. Así, según lo que expone en su obra, la identidad también es una necesidad afectiva («sentimiento»), cognitiva («conciencia de sí mismo y del otro como personas diferentes») y activa (el ser humano tiene que «tomar decisiones» haciendo uso de su libertad y voluntad).

En la tabla 1 se recoge un resumen de los elementos clave que ayudan a entender en qué consiste la identidad humana.

Tabla 1. Elementos clave de la identidad humana

La identidad humana es lo que define a la persona y la distingue frente a los otros
Se construye plenamente en función de las condiciones de la propia persona pero también de los hechos y las experiencias vividas: • Relaciones con los otros (cruce individuo-grupo-sociedad) • Historia de la propia vida • Historia social
La identidad humana solo se realiza en función de la interacción con el medio externo
Evoluciona a lo largo del tiempo
La necesidad de un sentimiento de identidad es vital e imperativa para el hombre

Fuente: elaboración propia.

Identificar a alguien implica, por lo tanto, reconocer cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona afectada.

En este sentido, la identidad física («el hecho de ser...») se manifiesta mediante señales biológicas, fisiológicas y de comportamiento, por lo que es razonable que algunas de ellas sean utilizadas por las autoridades públicas para ser registradas y así identificar a los individuos. En el caso de los documentos oficiales que certifican la identidad de una persona, como es el caso del documento nacional de identidad (DNI) en España, se seleccionan aquellas características que permiten discernir la identidad de forma inequívoca, intemporal e incondicional y que, sobre todo, conllevan un proceso de registro y comprobación rápido y barato. En concreto, combinan en el mismo documento características morfológicas y fisiológicas que ofrecen, de forma sencilla, una garantía razonable de que su portador es quien pretende representar y típicamente está formado por una fotografía, la huella dactilar y la firma manuscrita.

La necesidad de un sentimiento de identidad es tan vital e imperativa que el hombre no podría estar sano si no encontrara algún modo de satisfacerla.

Por supuesto la identidad, en sentido amplio, no se reduce a una huella dactilar asociada a un nombre y unos apellidos, sino que forman parte de ella también los rasgos antropomórficos, fisiológicos y psicosociales, como un todo. Además, en la vida diaria las personas, de manera consciente o inconsciente, presentan una u otra faceta de su identidad, por lo que la identidad social se manifiesta como un poliedro con muchas caras.

Sin duda, la identidad es una realidad compleja en construcción y evolución permanente. Así pues, es razonable que la realidad digital impacte de lleno en ella y tenga que ser objeto de estudio obligado.

Capítulo 2

La identidad digital

2.1 Componentes de la identidad digital

Tal y como se ha comentado en el capítulo anterior, la identidad es el conjunto de rasgos que nos individualizan y permiten distinguir a una persona de otra confirmando que esta es realmente quien dice ser, ya sea en el ámbito legal, familiar, digital, etc.

Hasta hace poco, configurar y gestionar la identidad personal era una tarea que comprendía tratar nuestra realidad en relación con las diferentes organizaciones y personas en un ámbito que tenía que ver únicamente con el entorno personal y físico más cercano. Sin embargo, la llegada de Internet de forma masiva a la vida de las personas y, sobre todo, la facilidad de interactuar y dejar huella en ella, hace que la gestión de la identidad se complemente con la realidad digital, que además incorpora nuevas características[1] que han de ser tenidas en cuenta por las personas para que la gestión de esa identidad sea realmente efectiva.

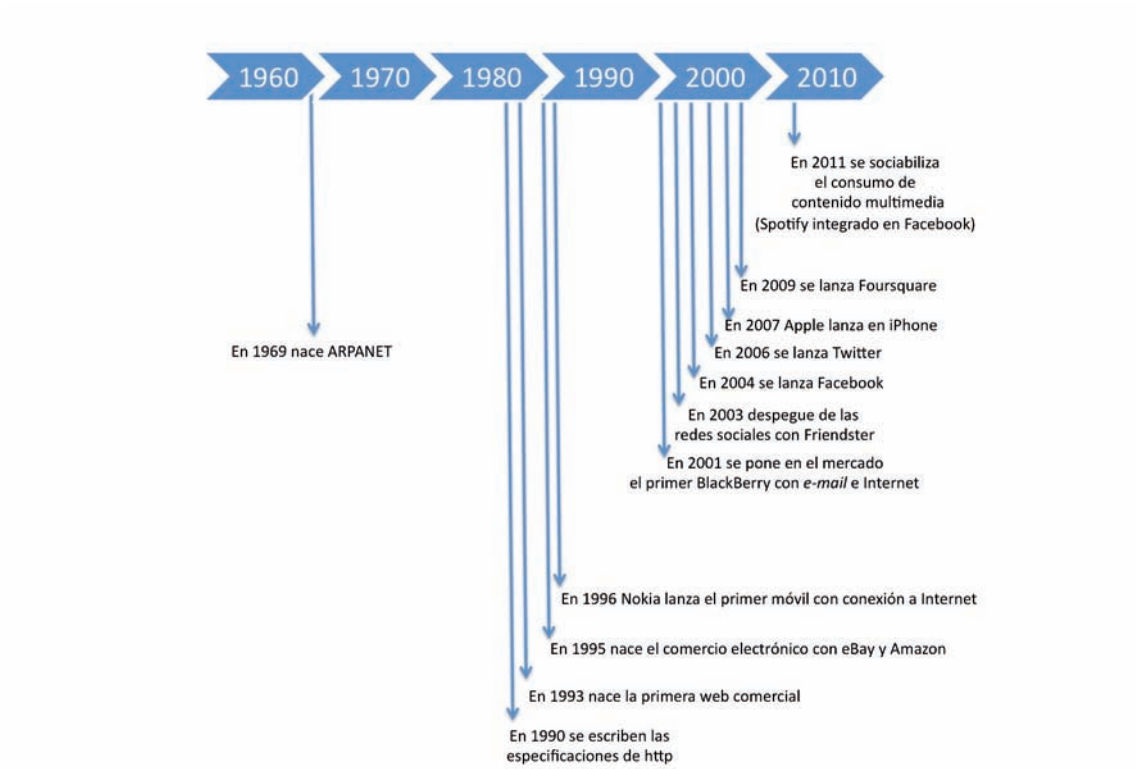
Durante los últimos 20 años el avance de la digitalización de las actividades de los ciudadanos y su migración hacia el medio *online* ha sido constante: se trabaja, se aprende, se compra, se vende, se llevan a cabo reuniones, se ven contenidos audiovisuales, se escucha audio, se invierte, se crea, se vota, se realizan donaciones...

Tal y como se recoge en la figura 1, durante la última década, las aplicaciones de carácter social han sido los principales motores de la evolución de Internet. Los usuarios tienden a compartir cada vez más aspectos de su vida y, además, cada vez en más servicios y sitios web. En la actualidad, es frecuente transmitir en directo (gracias al paradigma *real time web*)[2] la vida (*lifestreaming*),[3] las conexiones, los pensamientos, los conocimientos, las relaciones, las opiniones, etc. Por otro lado, los usuarios usan cada vez más dispositivos para conectarse a la Red, lo que también complementa la información sobre la identidad digital.

En resumen, toda la actividad de las personas en la Red es susceptible de ir configurando la identidad digital, puesto que deja un rastro fuerte y claro en ella, de manera consciente o inconsciente[4].

1. La huella que las personas dejamos en la Red es potencialmente permanente, puede ser enlazada, sigue un orden cronológico claro y, en muchas ocasiones, no puede ser borrada porque es información que ha sido compartida con otros.
2. Para mayor información, consultar el monográfico sobre el tema *Real Time Web: una nueva conciencia global*. Fundación Telefónica, 2011.
3. Concepto que se refiere al uso de las herramientas 2.0 para ir narrando la propia vida, en este caso relativa a la actividad realizada en Internet.
4. Gamero, Ruth, *La configuración de la identidad digital,* Nota Enter-IE 131, junio 2009.

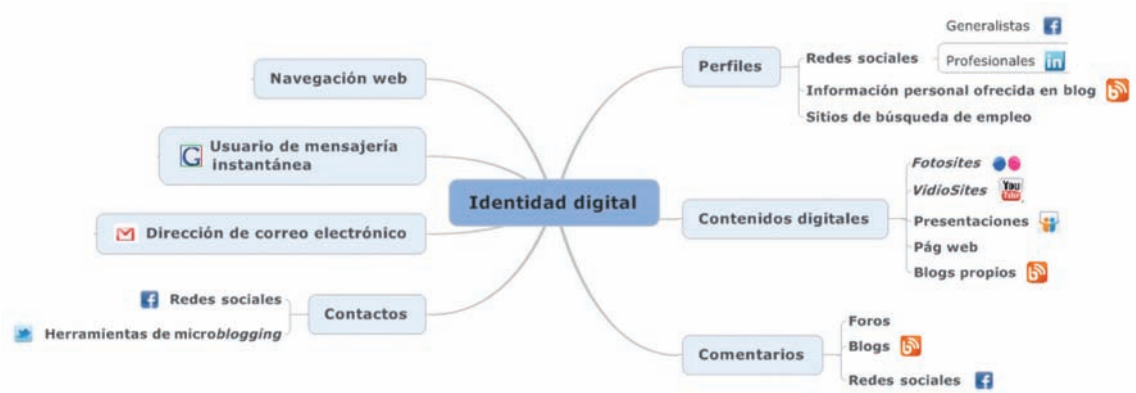
Figura 1. Hitos en la evolución de Internet



Fuente: elaboración propia.

En la figura 2, a modo de ejemplo, se muestra un conjunto de estos impactos en la Red que ayudan a esta configuración. En concreto, se trata de servicios y aplicaciones, como las redes sociales, los servicios de almacenamiento de datos, ya sean *fotosites*, *videosites*, blogs, foros, etc., las relaciones que se establecen, los círculos de confianza en los que se inserta la persona, los perfiles personales, etc.

Figura 2. Ejemplo de impactos en la Red que conforman la identidad digital



Fuente: elaboración propia.

El concepto de identidad digital es, pues, muy amplio, y está formado por muchos componentes que lo van configurando a lo largo del tiempo.

Según el modelo planteado por F. Georges,[5] la identidad digital está constituida por diferentes tipos de datos según el usuario tenga o no la intención de revelarlos, lo que da lugar a una identidad declarada, compuesta por aquella información que revela expresamente la persona, otra identidad actuante, según las acciones que esta lleva a cabo, y otra calculada o inferida, según el análisis de las acciones que realiza la persona. Toda esta información puede ser utilizada para configurar una idea de quién es y qué le gusta a una persona determinada.

En concreto, el tipo de datos que ayudan a configurar esta identidad pueden catalogarse como:

- Datos de identidad individual: se trata de identificadores como el nombre, el número de la Seguridad Social o el DNI, el número del permiso de conducción, el número de la tarjeta de crédito, la fecha de nacimiento, los identificadores sociales de los sitios web a los que accede, etc.
- Datos de comportamiento: sobre transacciones, historial de navegación, datos de localización, transcripciones del *call-center*, historial de compra, accesos, etc.[6]
- Datos derivados o calculados: son atributos modelados de manera analítica que sirven para hacer un perfilado de las personas, por ejemplo, para valorar el riesgo de un cliente a la hora de darle un crédito, entender la propensión a hacer algo, valorar su influencia en un ámbito determinado, etc.

5. http://fannygeorges.free.fr/
6. Estos datos son susceptibles de ofrecer una visión de la persona que supera, con mucho, el conocimiento que esta tiene de sí misma, pues permite un análisis de tendencias, comportamientos, influencias, secuencias... originadas en el comportamiento y en el creciente flujo de información que se comparte. También se denominan *shadow data*.

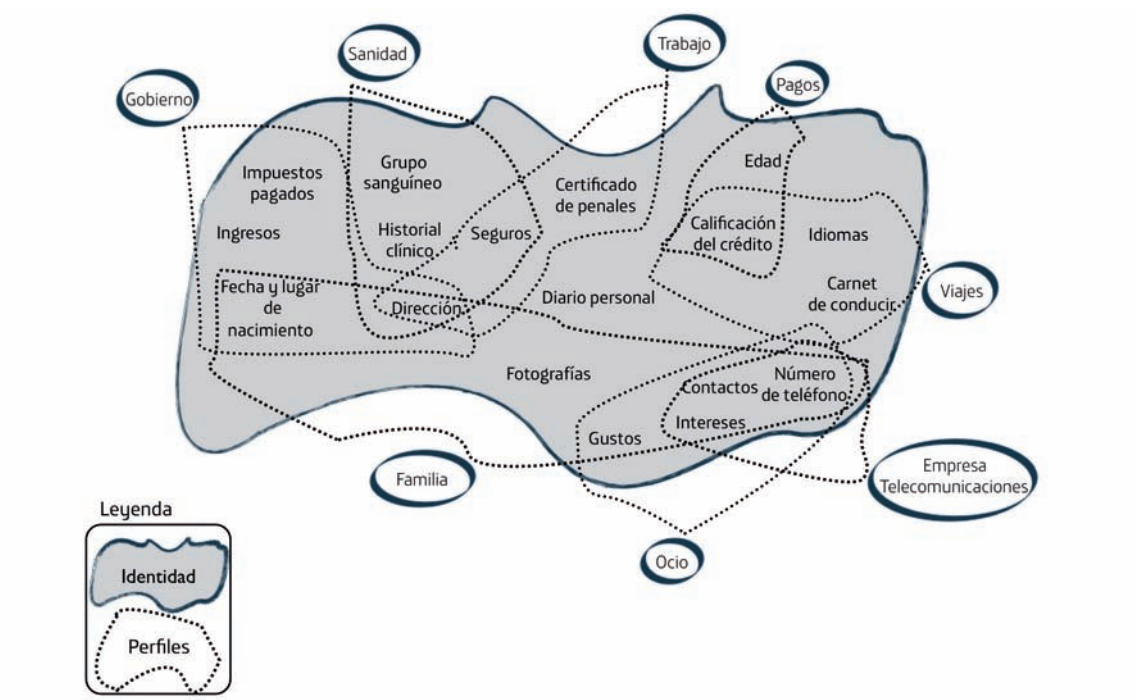
- Datos que va creando el propio usuario para identificarse: como opiniones sobre productos, redes profesionales a las que pertenece, «me gusta» en redes sociales, intenciones de compra, valoraciones y revisiones de productos, respuestas en foros, etc.

El concepto de identidad digital tiene, además, diferentes representaciones en distintos entornos, es decir, las personas cuentan con varios perfiles según el contexto en el que se desenvuelvan, perfiles que incluyen distinta información. Por ejemplo, la información que necesita un centro médico sobre un paciente cuando ingresa por una dolencia es diferente de la que requiere una tienda para que pueda dar por válida una compra, o de la que tienen los amigos sobre una determinada persona (figura 3).

Identidad digital, información, privacidad y seguridad son aspectos que van muy unidos, pues para gestionar correctamente la primera hay que poder gestionar los otros tres aspectos.

En este sentido, identidad digital, información, privacidad y seguridad son aspectos que van muy unidos, pues para gestionar correctamente la primera hay que poder gestionar los otros tres aspectos.

Figura 3. Ejemplo de datos de los diferentes perfiles de la identidad digital



Fuente: elaboración propia.

De manera genérica, tal y como se enumera en la tabla 2, la identidad digital es, pues, un concepto social, porque soporta los procesos de interacción de las personas; es subjetiva, ya que también intervienen en el proceso de identificación otros individuos que incorporan su subjetividad en la interpretación, por lo que diferentes personas podrán construir distintas «identidades» asociadas a la misma persona; tiene valor, pues permite la realización de transacciones; es referencial, pues no es la persona en sí, sino una referencia a ella; es crítica, pues su uso por terceros puede implicar

riesgos para la persona, así que su gestión se hace necesaria; es un concepto compuesto, ya que está formada por varios elementos procedentes tanto de la propia persona como de terceros y en algunos casos incluso sin su conocimiento o participación; es un concepto dinámico, que evoluciona con el tiempo; es contextual, pues los datos dependen del ámbito en el que la persona se desenvuelva en un momento dado, de hecho, las personas deben gestionar estos diferentes perfiles de su vida e incluso mantenerlos separados, pues el no hacerlo puede incluso implicar riesgos para ellos mismos. Por otro lado, la información registrada sobre las personas se puede conservar idealmente de manera permanente y, por lo tanto, se puede acceder a ella atendiendo incluso a un orden cronológico claro. El hecho de que gran parte de esa información sea compartida con otros hace que tampoco pueda ser eliminada. Finalmente, conviene recordar que la identidad digital es inexacta, ya que el proceso de identificación completo puede estar sujeto a errores.

Tabla 2. Características de la identidad digital

Social	Soporta los procesos de interacción social de las personas
Subjetiva	El proceso de identificación incorpora la subjetividad de las otras personas
Con valor	Permite la realización de transacciones que no serían posibles sin ella
Referencial	Se trata de una referencia a la persona
Crítica	Su uso por terceros puede implicar riesgos para la persona
Compuesta	Formada por varios elementos, tanto procedentes de la propia persona como por otros
Dinámica	Está siempre cambiando e incorporando nuevos elementos
Contextual	Según el contexto en el que se desenvuelva la persona, el perfil de la identidad digital tendrá una información u otra
Permanentemente accesible y ordenada cronológicamente	La información registrada sobre la persona se puede conservar y, por lo tanto, se puede acceder a ella de manera permanente. De hecho, en muchas ocasiones la información no puede ser borrada porque ha sido compartida con otros Por otro lado la información queda almacenada siguiendo un orden cronológico claro
Inexacta	El proceso de identificación siempre está sujeto a errores, algo que conviene tener muy en cuenta

Fuente: elaboración propia.

En resumen, las TIC (tecnologías de la información y la comunicación) crean una identidad expandida en la mayoría de sus usuarios, potencian sus habilidades y los capacitan para estar en contacto con otros con diferentes niveles de relación, intimidad, compromiso, etc.[7] Gracias a la vida digital, es posible conocer mejor a los otros, al mismo tiempo que es más fácil darnos a conocer, compartir con otros más cosas, tener más información y, en definitiva, gestionar mejor las relaciones sociales y la propia identidad real.[8]

Gracias a la vida digital es posible conocer mejor a los otros, al mismo tiempo que también es más fácil darnos a conocer.

2.2 El papel de la identidad digital en el comportamiento humano

Tal y como se ha comentado, la participación de la persona en el universo digital la complementa, ya que las herramientas *online* amplían las posibilidades y dotan a las personas de nuevas capacidades. Gracias a esta interacción es posible ser más fluido, variado, rico... porque todas las posibilidades que ofrecen las tecnologías y la posibilidad de estar conectado permanentemente hacen posible llegar a más.

En este sentido, el concepto de identidad se hace múltiple, fluido, distribuido y heterogéneo. Incluso el concepto que cada persona tiene de sí misma se integra como una pieza más en una red más amplia que es donde cobra sentido. Y es que cuando se incorpora la informática ubicua al individuo de manera permanente cambia el propio sentido de uno mismo. Incluso muchos objetos digitales terminan siendo extensiones de la construcción mental de un pensamiento.[9]

La experiencia digital y *online* del usuario es cada vez más rápida e inmersiva, las comunicaciones se hacen cada vez más bidireccionales y masivas, y la conexión en tiempo real (tanto a la información como a otras personas) hacen que gran parte de las actividades se conviertan en una experiencia atrayente, absorbente e incluso adictiva.[10] Este nuevo paradigma, conocido como *real time web*,[11] ofrece la posibilidad de disponer de un flujo de información constante y en tiempo real de cada una de las personas, de lo que estas piensan, sienten, hacen o crean, y ello contribuye, sin duda, a configurar esta identidad digital que es parte de la identidad de los seres humanos. Incluso, dando un paso más, este nuevo entorno contribuye a cambiar la propia identidad, por la influencia que tiene en la manera en la que se socializa, por los cambios que produce en el modo en el que se concibe la privacidad y también por cómo altera la atención de las personas.

De manera genérica, se puede afirmar, además, que Internet cambia dimensiones como el espacio y el tiempo y, por lo tanto, modifica sustancialmente el entorno. La Red acerca múltiples realidades de manera casi inmediata y en este sentido la distancia física se elimina, con lo que la posibilidad de acceder a casi cualquier conocimiento, información o persona de manera instantánea cambia notablemente la realidad. Por otro lado, en la Red, los hechos quedan ordenados temporalmente tal y como sucedieron, por lo que los recuerdos pueden quedar en cierto modo inalterados. En

7. Varela, Juan. http://periodistas21.blogspot.com/
8. Freire, Juan. http://nomada.blogs.com/jfreire/
9. Para profundizar en el tema de la identidad en Internet, consultar el trabajo de Sherry Turkle.
10. Al parecer, estos mínimos paquetes de información activan mecanismos cerebrales de recompensa como la dopamina, que están implicados en algunas adicciones.
11. Para abundar en este tema, consultar el monográfico *Real Time Web: una nueva conciencia global*, de Fundación Telefónica, 2011.

el mundo físico los recuerdos están asociados a una emoción y, por lo tanto, sujetos a un orden subjetivo. De hecho, el que los recuerdos no estén solo en nuestros circuitos cerebrales, sino que también se almacenen en el soporte digital que los conserva ordenados tal y como sucedieron, condiciona que el proceso de olvido y distorsión de los recuerdos no se lleve a cabo de la misma manera, por lo que influye directamente en nuestra memoria.

2.2.1 Cambios en los procesos de socialización

Nunca hasta ahora había sido posible relacionarse tanto y con tantas personas al mismo tiempo. Las posibilidades que ofrece el mundo digital son increíbles; este amplía nuestras limitaciones físicas y facilita un contacto cada vez más cercano y permanente con las personas que queremos. De hecho, se habla de las redes sociales como verdaderas herramientas de amplificación de las relaciones. Al mismo tiempo, ayudan a ampliar los círculos de conocidos, y expanden el grafo social con diferentes fines (profesionales, formativos, de ocio, etc.).

Además, la forma en la que se socializa, en la que la gente se comunica y colabora se está transformando profundamente. Las comunicaciones se hacen cada vez más rápidas, directas e instantáneas. La vida digital tiene un alto potencial de ampliación de la experiencia humana. De hecho, las relaciones que se mantienen pueden superar barreras como el tiempo, la distancia e incluso el idioma. La experiencia *online* ofrece también la posibilidad de «engancharse» a lo que otras personas hacen, sienten o experimentan. El mundo se interconecta cada vez más y se hace más comprensible porque es más fácil acceder al contexto de otras personas.

2.2.2 Cambios cognitivos

La actividad de las personas en la Red, sobre todo la que tiene que ver con el acceso en tiempo real a la información y la comunicación con otras personas, tiene su coste y ese es precisamente el de la atención. En un entorno en el que la información fluye continuamente, la atención sufre, de hecho se habla de la *continuous partial attention*,[12] entendida como una atención parcial que se tiene, además, de manera continua a lo largo del tiempo.[13]

La vida en red ofrece cada vez más opciones para acceder y adquirir conocimiento, pero bajo una aproximación diferente a la tradicional, ya que las interrupciones, la lectura no secuencial y el contenido disperso hacen que la atención se vea modificada. La multitarea, instigada por el uso de Internet, cambia los modelos cognitivos, por lo que puede convertir a las personas en seres más eficientes procesando información pero con el riesgo de ser también más superficiales e incluso más uniformes.[14] La utilización de Internet como un disco duro en el que almacenamos recuerdos permite que no se realice esfuerzo en memorizar información lo que, según algunos expertos, puede suponer una merma de capacidades, mientras otros lo consideran un aspecto positivo ya que estos recursos que antes se dedicaban a memorizar, se pueden dedicar ahora a otras actividades.

---

12 Linda Stone introdujo el concepto en 1998.

13 En este sentido, hay que destacar la iniciativa de «El día Isma» (http://www.youtube.com/watch?v=S_05_gtr4Mw), una reciente campaña de publicidad que habla de cómo intentamos atender tantos estímulos al cabo del día que finalmente no hacemos caso como deberíamos a ninguno de ellos.

14 Según Nicholas Carr.

Otros cambios que se cree que Internet produce en nuestra forma de procesar la información se refieren al aumento de la capacidad de filtrar información, que se desarrolla como respuesta al crecimiento exponencial de la cantidad de información a la que somos expuestos, e incluso hay quien afirma que produce un incremento de la actividad cerebral con cambios en los circuitos neuronales.[15]

2.2.3 Cambios en el concepto de privacidad

Gran parte de las aplicaciones y servicios digitales que utilizan las personas albergan información personal muy valiosa sobre ellas. Esta información es compartida con otros y ello está configurando un entorno en el que el concepto de privacidad e intimidad está evolucionando.

Los medios sociales permiten, además, compartir datos de la vida de las personas con un mayor número de contactos y hacerlo de manera permanente y trazable. La intimidad es un concepto en evolución que cada vez se hace más público y, por otro lado, menos gestionable por la propia persona. En la actualidad, es habitual que las personas compartan información sobre las actividades que realizan en un determinado momento, fotos, vídeos, comentarios o información de geolocalización y esta información, una vez compartida, entra en el «flujo» de información y puede distribuirse libremente, por lo que la gestión escapa del control de la persona que la compartió. Los límites son cada vez más difusos y cada vez es más difícil encapsular una información que es fluida por naturaleza y fluye aún más en los ecosistemas de redes digitales.[16]

Ante este escenario, la gestión de la privacidad se convierte en un tema esencial para el futuro y para la gestión de la propia identidad digital. Es preciso, pues, que el propio usuario sea el que tenga el control sobre la compartición de sus datos y que, por lo tanto, se requiera siempre su consentimiento en las operaciones relacionadas con su identidad. Por otro lado, es necesario también poder distinguir entre diferentes perfiles, públicos y privados, para compartir según qué información interese en cada momento. La gestión de la privacidad, como la gestión de la identidad digital, será una tarea a la que las personas tendrán que dedicar especial atención en su relación con los medios sociales porque en ellos, además, irá implícita su reputación. Un cambio notable que se está produciendo en este sentido es que, si bien hace unos años las personas decidían qué aspectos de la privacidad hacían públicos, en la actualidad, se trata de decidir qué preservar para así trabajar activamente para conseguirlo.

En este sentido la Dra. Danah Boyd,[17] experta en el ámbito de identidad digital y en el uso de redes sociales por parte de jóvenes, explica que el concepto de privacidad ha ido evolucionando notablemente a lo largo de los últimos años. De hecho, en la actualidad, los jóvenes consideran que Internet es por defecto público y todo lo que hacen allí tiene este carácter, con lo que establecen estrategias para hacer privadas ciertas conversaciones. Además, esta investigadora destaca la necesidad de que los diferentes sistemas que ayuden a gestionar la identidad digital deben estar diseñados para satisfacer las necesidades de control de la información de los usuarios, trasladando al mundo telemático los protocolos de intercambio de información de identidad usados por los seres humanos en las interacciones sociales.

15. Gary Small.
16. Dolors Reig. http://www.dreig.eu/caparazon/
17. http://www.danah.org/

En resumen, la gestión de la identidad tiene mucho que ver con el valor que las personas dan a su privacidad y a cuánto estén dispuestas a ceder a cambio de la comodidad y de los posibles beneficios informativos y comerciales que ofrezcan servicios del nuevo ecosistema digital.

2.2.4 Cambios en el concepto de reputación social

Tal y como ya se ha comentado en el informe, el control y la gestión de la información personal en la Red tiene unas características diferentes que en cualquier otro medio. Por una parte, la facilidad con la que la información se replica en diferentes servidores, y por otra, la dificultad del usuario para seguir el ciclo de vida de dicha información, han contribuido a crear una conciencia entre la población acerca de la importancia de gestionar esta información y en concreto la reputación en la Red.

Dadas las dificultades que los usuarios encuentran para hacer personalmente un seguimiento de la información que circula sobre ellos en la Red, han ido apareciendo en los últimos años servicios que tienen como objetivo el seguimiento de esta información, y además incluyen herramientas para conseguir mejorar la reputación. Algunos ejemplos de este tipo de empresa son Reputation.com, Internetreputation.com o la española Webrunner (figura 4). Estas herramientas están dirigidas tanto a usuarios particulares como a empresas que quieran conocer cuál es su reputación en la web o mejorar su huella en este medio.

Figura 4. Servicios de seguimiento y creación de reputación en Internet

Otro ejemplo es el de la empresa connect.me, que cuenta con una herramienta que permite a los usuarios verificar la información de otros usuarios con el fin de darle más veracidad a los perfiles en redes sociales como Facebook, Twitter o LinkedIn.

En concreto, el funcionamiento es el siguiente: un usuario de Facebook, Twitter o LinkedIn puede crear una tarjeta en connect.me en la que únicamente rellenará sus gustos, aficiones, tipo de trabajo, etc. De la misma manera, una vez rellenada su tarjeta propia, el usuario deberá indicar o «avalar» cuáles cree que son los gustos, intereses, trabajos, etc. de algunas de las amistades de

dichas redes sociales. De este modo, según vayan coincidiendo ambas versiones irá aumentando el nivel de veracidad de un usuario. En este sentido, hay varios tipos de niveles de veracidad:

1. Usuario sin verificar: usuario que simplemente está registrado.
2. Usuario verificado: que ha avalado a más de diez personas y ha sido avalado por más de tres.
3. Usuario de confianza: que ha avalado a más de 25 personas y ha sido avalado por más de 25.
4. Anclaje de confianza: un usuario de confianza que ha sido avalado por tres usuarios que son anclaje de confianza.

Por último, connect.me permite compartir la tarjeta con las etiquetas que ha completado la persona y con la que se puede conocer a personas con los mismos intereses (figura 5).

Figura 5. Funcionalidades de connect.me

Otro ejemplo es Secure.me, que permite a los usuarios supervisar los contenidos de Facebook incluyendo la localización de fotos de las personas aunque no se esté etiquetado. Se trata de otro servicio que ofrece soporte a la gestión de la reputación *online* (figura 6).

Secure.me analiza en profundidad las actividades del usuario, actualizaciones de estado, comentarios, «me gusta» y mensajes con información de ubicación. La aplicación puede realizar estas acciones debido a que los usuarios dan permiso a Secure.me para ver todos los datos de Facebook, independientemente de la configuración de privacidad empleada.

Por otro lado, la compañía también utiliza la tecnología de reconocimiento facial para escanear fotos en el círculo de amigos de un usuario para chequear si este está presente en dichas imágenes. Facebook notifica a los usuarios por correo electrónico si son etiquetados en las fotos. Pero si no lo están, los usuarios tienen que leer con cuidado los perfiles de sus amigos para ver si están

presentes en ellas. Por ello, si Secure.me encuentra una foto que no está etiquetada, la marcará de manera especial para que el usuario pueda verla. Se trata, en definitiva, de tener herramientas que permitan controlar lo que otros dicen o dejan ver de nosotros en la Red.

Figura 6. Secure.me

2.2.5 Cambios en nuestras relaciones con las administraciones: e-ciudadano

Si desde hace ya unos años se habla de la e-Administración como aquella administración en la que los procedimientos han evolucionado hacia el soporte *online*, en la actualidad, como consecuencia directa de este fenómeno, podemos hablar de los e-ciudadanos. Se trata de la otra cara de esta evolución, en la que el foco se pone en el ciudadano como protagonista de la sociedad y, por tanto, de la relación con las administraciones. Nuevas tecnologías de autenticación y validación de datos, así como nuevos paradigmas que han ido calando en la Administración, como el Open Data, han supuesto el caldo de cultivo para esta nueva situación. Se trata de un fenómeno que permite que el ciudadano sea aceptado en su versión digital con la misma validez que en persona, lo que facilita en muchos casos la prestación de los servicios e incluso permite hablar de un empoderamiento del ciudadano, que puede participar de forma más activa en las decisiones que le afectan de alguna manera. Un ejemplo de buena aplicación de este concepto sería el de la ciudad de Singapur, donde se ha llevado a cabo una iniciativa ambiciosa bajo la filosofía «centrado en el ciudadano». El portal eCitizen[18] (figura 7) permite el acceso a los servicios, aplicaciones útiles para el ciudadano como un planificador de rutas, así como un tablón de anuncios o la posibilidad de centralizar todas las co-

18. http://alpha.ecitizen.sg/

municaciones con la administración, sustituyendo de esta manera al correo físico. Se trata, por tanto, de un nuevo modelo de relación mayor y más fácil en el que la comunicación con el ciudadano es constante. Nuevas tendencias como ciudades inteligentes, movimiento Open Data y el desarrollo de nuevos servicios móviles serán los motores de este cambio en el futuro.

Figura 7. Portal eCitizen Singapur

2.3 Construcción de la identidad digital

Tal y como se ha comentado, las nuevas tecnologías pueden ser un determinante esencial a la hora de configurar quién y cómo es una persona. Esta afirmación, en el caso de los jóvenes, ya es una realidad, como señalan recientes estudios.[19] De hecho, valoran y dedican tiempo a la construcción y gestión de una identidad «pública virtual» que requiere una comunicación «más visual», con fotos y vídeos como principales materiales constructivos. Además, hacen uso de una comunicación «más fluida» que multiplica las relaciones y los momentos de interacción (figura 8).

19. 6.º Observatorio de Tendencias de Nokia sobre «los jóvenes, los móviles y la tecnología».

Esta generación continuamente gestiona su identidad, mediante técnicas como el *story telling* (contar una historia) o el *life casting digital* (retransmisión de la vida en formato digital). En este proceso, los límites entre lo público y lo privado se están redefiniendo permanentemente. Por otro lado, utilizan los diferentes medios de comunicación (voz, redes sociales, mensajería instantánea, correos electrónicos, etc.) para modular el grado de intimidad de las comunicaciones. Se trata de una generación que requiere el estímulo constante y necesita rellenar cualquier tiempo de espera o tiempos muertos haciendo algo. Para ellos, la Red es una realidad envolvente, omnipresente, que les abre un mundo de fantasía y les permite comunicarse y acceder a la información con inmediatez y comodidad al mismo tiempo que les permite divertirse y definirse con estilo. Sin duda, es una herramienta que les confiere poder y, por lo tanto, la valoran.

Figura 8. La tecnología y los jóvenes: construcción de la identidad digital

Fuente: 6.º Observatorio de Tendencias Nokia: «Los jóvenes, los móviles y la tecnología».

El estado actual de la web social hace posible que las personas vayan construyendo una identidad en red cada vez más madura, transparente y aumentada. Además, con las nuevas herramientas es posible conocerse, expresarse y realizarse en los procesos de interacción en las redes sociales. Sin duda, se abre un mundo de nuevas posibilidades para la construcción, no solo de la identidad digital, sino de la propia identidad como persona.[20]

20. Dolors Reig. http://es.scribd.com/doc/74794642/identidades-digitales

Capítulo 3

La actitud de los usuarios ante la gestión de la identidad digital

Internet se ha convertido en un elemento esencial en la vida de las personas. Según un reciente estudio, el 50 % de los estudiantes y el 48 % de los jóvenes profesionales españoles en activo consideran Internet un recurso tan vital como el aire, el agua, la comida o la vivienda.[21] El nivel de uso de la Red ha ido en aumento en los últimos años; en efecto, según datos de 2011, el 71,4 % de los internautas en España son ya intensivos,[22] lo que supone que 16,6 millones de personas acceden a diario a Internet. Y entre las actividades que más han crecido, sin duda están las relacionadas con la actividad social, como las redes sociales, que hoy por hoy se han convertido en habituales entre un alto porcentaje de la población.

La preocupación por la gestión de la privacidad es el principal motor de la gestión de la identidad digital.

La vida de las personas está experimentando un proceso de digitalización, tanto en lo que se refiere a sus actividades, a los contenidos que se gestionan y a los que se accede, como a las relaciones que se establecen y mantienen con otras personas. Este proceso está produciendo una explosión de datos que inunda el mundo digital. Datos que, en cierta medida, ayudan a identificar a la persona, en todos sus perfiles o roles: cliente, usuario, contribuyente, estudiante, paciente, empleado, inversor, espectador, audiencia, etc. En este ámbito es razonable que las personas estén adquiriendo una conciencia más clara de la necesidad de disponer del control respecto a la privacidad y la seguridad de sus datos, además de controlar de algún modo la información que se almacena y se comparte sobre ellos. De hecho, según un reciente estudio, el 61 % de los internautas estadounidenses pagaría por el contenido a cambio de mantener su privacidad.[23] En realidad, esta preocupación por la gestión de la privacidad es el principal motor de la gestión de la identidad digital.

En la actualidad, el consumidor se ha convertido en un producto. Plataformas como Google, Facebook, Foursquare y Twitter son las nuevas plantas de producción, y el usuario *online*, que deja un rastro digital por el ciberespacio cuando navega por Internet y participa en las redes sociales, genera datos que pueden ser comprados y vendidos con el objetivo de que ciertas empresas mejoren su oferta al consumidor.

Por otro lado, las empresas tradicionales también han descubierto que pueden crear nuevas líneas de negocios mediante la recogida y la utilización de información sobre el consumidor.[24]

De hecho, supermercados, gasolineras y otros minoristas ofrecen ya desde hace tiempo tarjetas de fidelidad que analizan las compras realizadas para ofrecer ofertas ajustadas a sus clientes.[25] Asimismo, a través de webs de medios sociales como Foursquare, las personas trasladan información de sus gastos en el mundo real al mundo virtual.

Es decir, el panorama actual configura un universo de datos ingente, tendencia que ha dado en denominarse Big Data y que implica el tratamiento y análisis de enormes repositorios de datos, tan desproporcionadamente grandes que resulta imposible tratarlos con las herramien-

21. Cisco. 2.º estudio anual sobre la mentalidad, las expectativas y el comportamiento de la próxima generación de jóvenes trabajadores ante la tecnología. Octubre, 2011.
22. INE, 2011.
23. Gallup, 2010.
24. Andrea Matwyshyn, profesora de Estudios jurídicos y de Ética en los negocios de Wharton.
25. Cabe destacar que la administradora de tarjetas Visa registró la patente de un método para el envío de publicidad *online* dirigida al consumidor basado, en parte, en sus gastos con la tarjeta de crédito física.

tas de bases de datos y analíticas convencionales. Sin duda, en un futuro próximo, las empresas que sean capaces de extraer conocimiento de esta información marcarán la diferencia respecto a las que no puedan hacerlo y, por tanto, el mejor competidor en una industria determinada será el que sea capaz de analizar mejor esta información y sepa tratarla de manera respetuosa, que no redunde en una sensación de «invasión» o de pérdida de privacidad de sus usuarios.[26]

El panorama actual configura un universo de datos ingente, tendencia que ha dado en denominarse Big Data y que implica el tratamiento y análisis de enormes repositorios de datos.

3.1 Los usuarios están preocupados por la protección de sus datos

La preocupación generalizada por la protección de los datos personales es un hecho. Según un reciente estudio realizado en el ámbito de la Unión Europea (UE), el 88 % de los encuestados declara que le gustaría ser informado en caso de que se perdieran, robaran o alteraran de cualquier forma aquellos datos personales suyos que estén en poder de terceros.

Esta preocupación se acrecienta a medida que salen a la luz incidentes como las intrusiones en los sistemas de información de empresas[27] que comprometen la seguridad de los datos de los clientes. Este es el caso de empresas como Epsilon, Sony, Citi, TripAdvisor/Expedia y RSA, que se han visto implicadas en este tipo de problemas, lo que ha supuesto además un alto coste para la credibilidad de su marca. Según estudios recientes, la media de coste de estas intrusiones para las compañías es de 214 dólares por usuario registrado.[28] En el caso concreto de la intrusión que sufrió Sony Online Entertainment en los datos de la PlayStation Network (PSN) en mayo de 2011, se estima que el coste ascendió a 171 millones de dólares, sin tener en cuenta los costes de las demandas que interpusieron muchos de los afectados.

Por otro lado, son también numerosas las polémicas en torno a la gestión de los datos personales en las que se están viendo implicadas las grandes empresas de Internet, como Google o Facebook, entre otras. En el caso de Facebook, por ejemplo, se le acusa de no tener una política clara en cuanto a la gestión de los datos de sus usuarios. En concreto, en verano de 2011 las agencias de protección de datos de diferentes países nórdicos (Noruega, Suecia, Dinamarca, Finlandia, entre otros) consideraron que era difícil para los usuarios navegar por la vasta cantidad de información y comprender plenamente el impacto real que tiene para su privacidad pertenecer a Facebook, y presentaron un listado de preguntas relativas al almacenamiento de información personal de los usuarios. Esta iniciativa fue promovida por las quejas del público referentes al uso que hace la red social de la información personal y de la puesta en común de información con otras empresas (imágenes, datos del muro, etc.).

Es razonable, pues, que en la actualidad ya se estén dando muchos pasos para atender estas demandas por parte de la sociedad. En concreto, en virtud de las nuevas normas de la UE aplicables desde el 25 de mayo de 2011, los operadores de telecomunicaciones y los proveedores de servicios de Internet tienen que tomar fuertes medidas de seguridad para proteger el nombre, la dirección electrónica y los datos de la cuenta bancaria de sus clientes, así como la información

26. Enrique Dans. http://www.enriquedans.com/2011/11/implicaciones-eticas-del-big-data.html
27. "What they know". The Wall Street Journal. http://online.wsj.com/public/page/what-they-know-digital-privacy.html
28. http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf

relativa a sus llamadas de teléfono y a sus sesiones de Internet. Las nuevas normas disponen también que, en caso de que se vulnere la seguridad o se pierdan o roben datos personales, los operadores informen inmediatamente a sus clientes y a las autoridades responsables de la protección de datos.[29] Es decir, las nuevas normas están restringiendo la manera en que los mercados capturan, almacenan y comparten los datos de los usuarios, incluso dentro de su propia organización.

Desde hace algún tiempo, el movimiento a favor de la privacidad digital está volviéndose cada vez más fuerte. En octubre de 2011, el presidente de la FTC (Comisión Federal de Negocios de Estados Unidos), acusó de *cyberazzi* a los recolectores de datos digitales y defendió la creación de un mecanismo que impidiera el seguimiento de datos, lo que ayudaría al consumidor a controlar mejor la información *online* compartida. Actualmente en EE. UU. la mayoría de los estados recogen en su legislación alguna norma relativa a la protección de la privacidad de los datos de los usuarios, así como a la transparencia en la recogida de datos.

Por otro lado, desde grupos de tecnología bien posicionados como Electronic Frontier Foundation, hasta nuevos grupos específicos de privacidad como la Privacy Rights Clearinghouse (defensores de la protección de los datos y de la privacidad del consumidor) se están llevando a cabo acciones para incrementar la conciencia de la necesidad de gestionar los datos relativos a la identidad digital y, por lo tanto, la privacidad de los mismos.

3.2 ¿Qué datos son importantes desde el punto de vista de la privacidad?

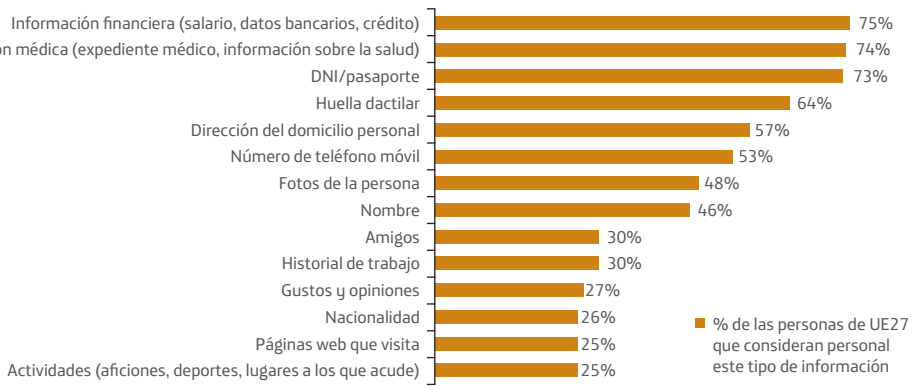
Tal y como se ha comentado, la identidad de un usuario en la Red está formada por una gran diversidad de información, que se encuentra distribuida en un amplio número de sistemas, empresas, organismos e instituciones.

Dependiendo de la naturaleza de estos datos, la percepción de los usuarios en cuanto al grado de privacidad de esta será diferente. Por ello, se puede encontrar desde información que los usuarios no perciben como datos excesivamente privados y cuyo conocimiento por terceras personas o empresas no es visto como un aspecto negativo, hasta datos que son considerados muy sensibles y, por lo tanto, no susceptibles de ser transmitidos o usados fuera del entorno originario.

Entre los datos que poseen para los usuarios un elevado grado de confidencialidad se encuentra la información financiera y la médica, consideradas por el 75 % y el 74 % de los europeos como información personal y, por lo tanto, que no debe ser accesible de forma directa por terceros. Mientras, en el otro extremo, se encuentran datos como la nacionalidad, los *websites* que se visitan o las actividades que se hacen en la Red, con un 25 % de usuarios que lo consideran como información de carácter personal (figura 9).

29. La *E-Communications Household Survey* (encuesta sobre las comunicaciones electrónicas en los hogares) se efectuó entre el 9 de febrero y el 8 de marzo de 2011, sobre una muestra de 27.000 hogares representativos de la población de la UE.

Figura 9. Tipos de información y datos que son considerados como información personal (UE)



Fuente: European Commission. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. Junio, 2011.

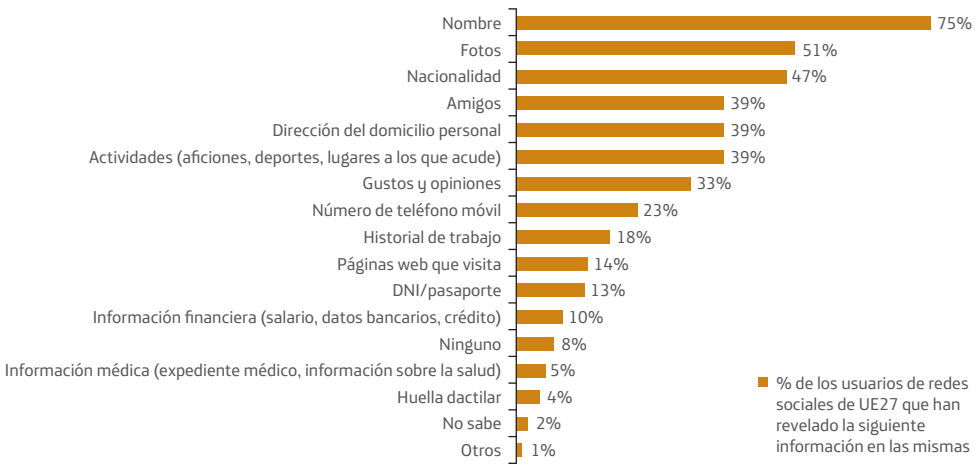
Por otro lado, se observa cómo la importancia que se otorga a la privacidad depende principalmente del nivel cultural de los usuarios y del grado de utilización de Internet, a mayor nivel cultural y a mayor grado de utilización de Internet, mayor es la conciencia que se va desarrollando con respecto a este punto.

3.3 ¿Cuál es la visión respecto a las redes sociales y los lugares de compra?

Tal y como se ha comentado, las redes sociales están pasando a formar parte, de manera muy importante, de la actividad que se realiza en Internet habitualmente. En ellas, el usuario utiliza un espacio personal en el que introduce información propia y se relaciona con otros contactos. Los datos introducidos por el usuario suelen ser el nombre propio, fotos, comentarios, gustos, amigos, etc. (figura 10).

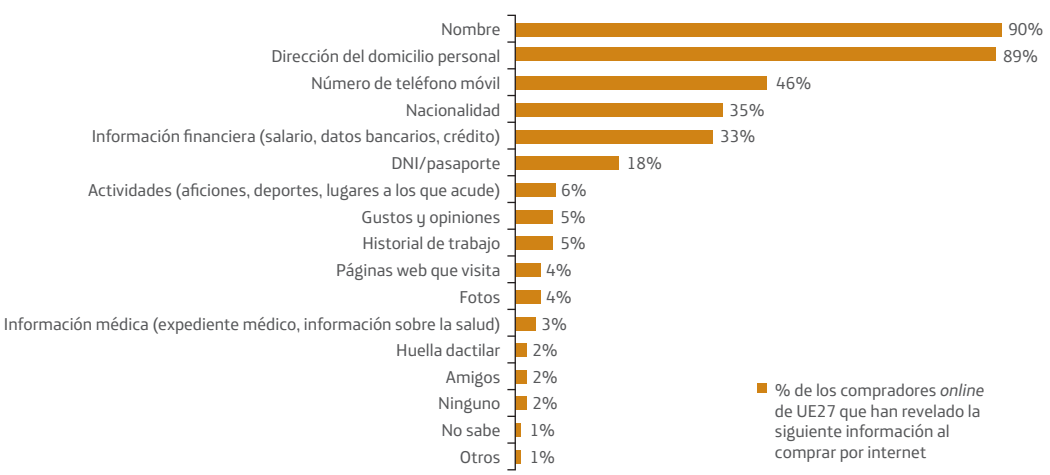
En el caso de las compras por Internet, la información que suele darse más habitualmente es el nombre y la dirección, con porcentajes cercanos al 90 %, seguida del número del teléfono móvil (46 %), la nacionalidad (35 %), así como la información financiera (número de tarjeta), con el 33 % (figura 11).

Figura 10. Tipo de información que se distribuye en sitios sociales y sitios de compartición de información (UE)



Base: Usuarios de redes sociales (40 % del total de la muestra).
Fuente: European Commission. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. Junio, 2011.

Figura 11. Tipo de información revelada en sitios de compra *online* (UE)



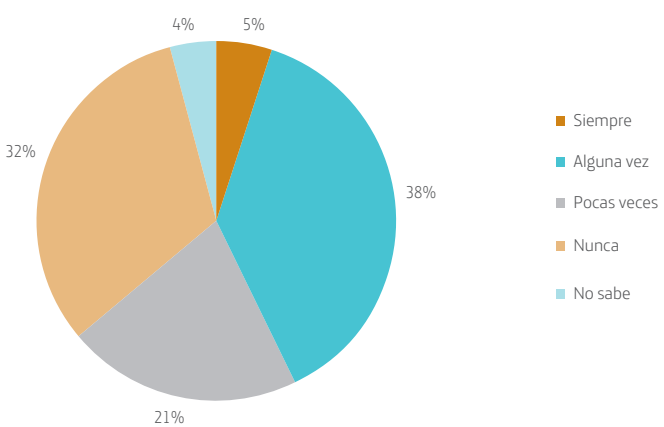
Fuente: European Commission. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. Junio, 2011.

3.4 Solo la información estrictamente necesaria

La preocupación de los usuarios por el uso de su información está haciendo también que cada vez más se establezcan principios para que las empresas u organizaciones usen solo la información imprescindible y necesaria del usuario para realizar los trámites o gestiones determinadas. Sin embargo, esta no es una práctica completamente extendida y tal y como se observa en la figura 12, es muy común que los ciudadanos introduzcan un volumen de información superior al estrictamente necesario para la prestación de un servicio: el 5 % de los usuarios en el ámbito de la UE afirma que siempre y el 38 % que en algunas ocasiones. En el caso de España, el 54 % de las personas afirman que en ocasiones han tenido que introducir una cantidad mayor de información que la necesaria en este tipo de herramientas.

Sin duda, es preciso que, en estas circunstancias, se reduzca la petición de información o que se explique de manera adecuada al usuario el motivo (porque se vaya a hacer un uso futuro de la información que le beneficie, etc.).

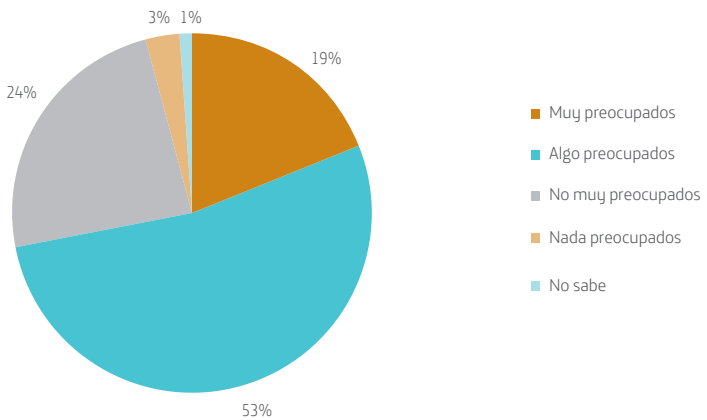
Figura 12. Solicitud de más información personal de la necesaria para acceder a algún servicio *online* (UE)



Fuente: European Commission. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. Junio, 2011.

Por otro lado, hay que tener en cuenta que el hecho de introducir más información de la necesaria para la prestación de un servicio determinado supone un motivo de preocupación para la mayoría de los usuarios (figura 13), que puede variar de una preocupación mayor (19 %), a una preocupación moderada (53 %).

Figura 13. Grado de preocupación por la introducción de más información personal de la necesaria (UE)



Fuente: European Commission. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. Junio, 2011.

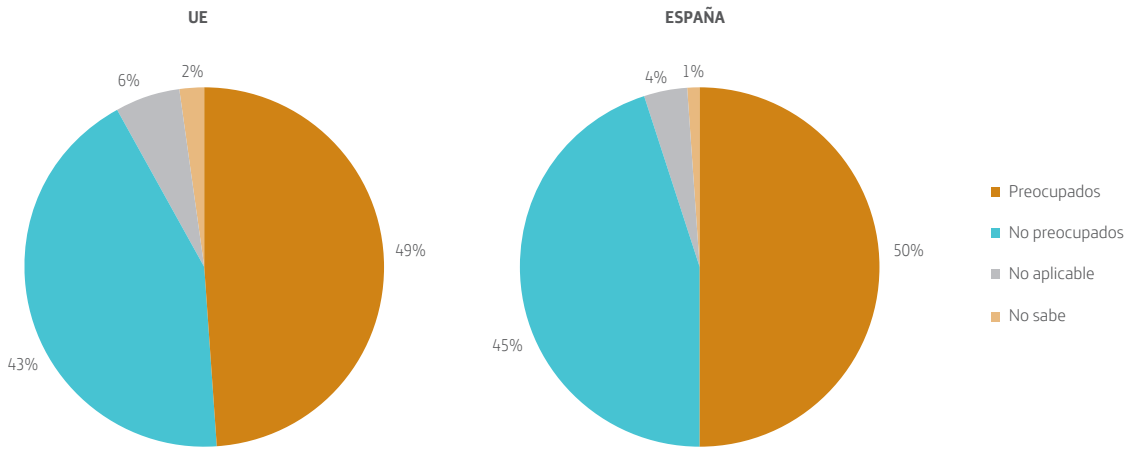
En el caso de las redes sociales, las principales preocupaciones respecto a la utilización de la información tienen que ver con el uso de la información sin el permiso explícito del usuario, la posibilidad de ser víctima de un fraude, y el hecho de que las empresas pasen su información a terceras empresas sin el consentimiento explícito del usuario.

3.5 Las particularidades de la movilidad en cuanto a privacidad

Otro tipo de información que también preocupa entre los usuarios tiene que ver con la que se genera en relación con la movilidad. Por una parte, es cierto que la mayoría de los usuarios están dispuestos a compartir información relativa a su posición para conseguir mejores servicios, aunque también este hecho crea un sentimiento de inseguridad.

En el caso de España, el 50 % de los usuarios muestran preocupación ante un posible seguimiento del contenido de las conversaciones o de su posición, cuando están utilizando dispositivos móviles. En Europa el grado de preocupación se sitúa en el 49 % (figura 14).

Figura 14. Grado de preocupación por el seguimiento y almacenamiento del comportamiento del usuario a través del móvil o Internet móvil (UE y España)



Fuente: European Commission. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. Junio, 2011.

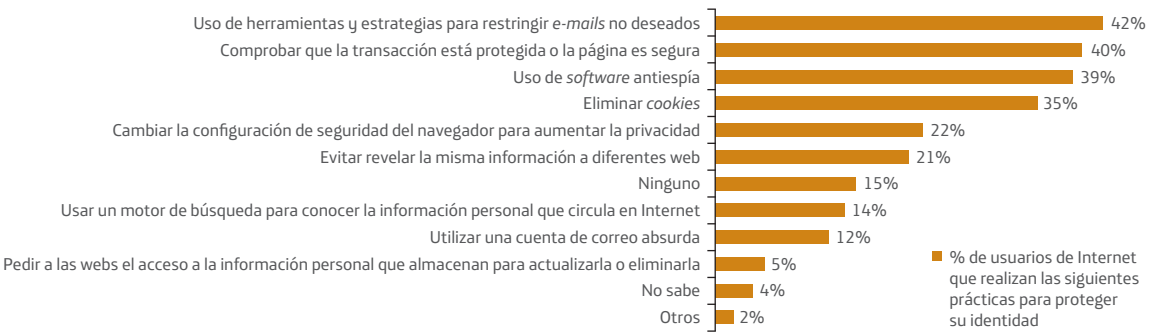
3.6 ¿Qué medidas toma el usuario con respecto a la privacidad tanto en Internet como en su vida diaria?

Además de las diferentes tecnologías que existen en el mercado orientadas a la seguridad y la protección de la privacidad, también es importante destacar la importancia que tiene la concienciación de que es necesario un comportamiento adecuado del usuario para prevenir malos usos futuros de la información personal.

La confianza y la credibilidad son aspectos clave en todo el ecosistema de identidad-privacidad-seguridad, y los usuarios tienden a tener diferentes grados de tolerancia a la hora de hacer frente a una situación en la que tengan que mostrar información propia en función de la empresa que lo solicite. De hecho, en la vida diaria, los usuarios ya toman determinadas medidas entre las que destacan el dar la mínima información posible (62 %), nunca desvelar claves secretas (56 %) y solamente desvelar información a aquellas personas o entidades en las que se tenga confianza (47 %).

En el campo de Internet, las acciones más utilizadas en este sentido son: disponer de herramientas para limitar *e-mails* no deseados (42 %), comprobar que las transacciones están protegidas o el sitio web donde se realiza la transacción tiene algún logo o etiqueta garantía de seguridad (40 %), el uso de *software* antiespía (39 %) así como el borrado de *cookies*, con el 35 % (figura 15).

Figura 15. Tareas realizadas en Internet para proteger la identidad (UE)



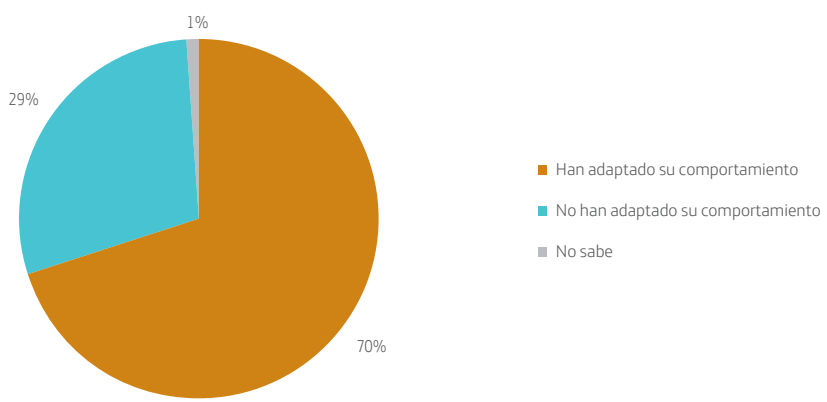
Fuente: European Commission. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. Junio, 2011.

3.7 Importancia de los términos de privacidad

Los servicios que requieren que el usuario introduzca información de carácter personal tienen siempre asociadas unas políticas reflejadas en los términos de privacidad que deben ser firmados por los usuarios a la hora de contratar o acceder a dichos servicios.

En muchas ocasiones, los usuarios no leen dichas condiciones y, por lo tanto, desconocen hasta qué punto pueden ser usados sus datos. En el caso de España, tan solo el 52 % de las personas leen dichos documentos, 6 puntos porcentuales por debajo de la media de la UE. No obstante, la mayoría de los usuarios que leen estas condiciones (el 70 %), sí que las tienen en cuenta de alguna manera y ello afecta a su comportamiento en la Red (figura 16).

Figura 16. Adaptación del comportamiento tras leer las políticas de privacidad



Fuente: European Commission. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. Junio, 2011.

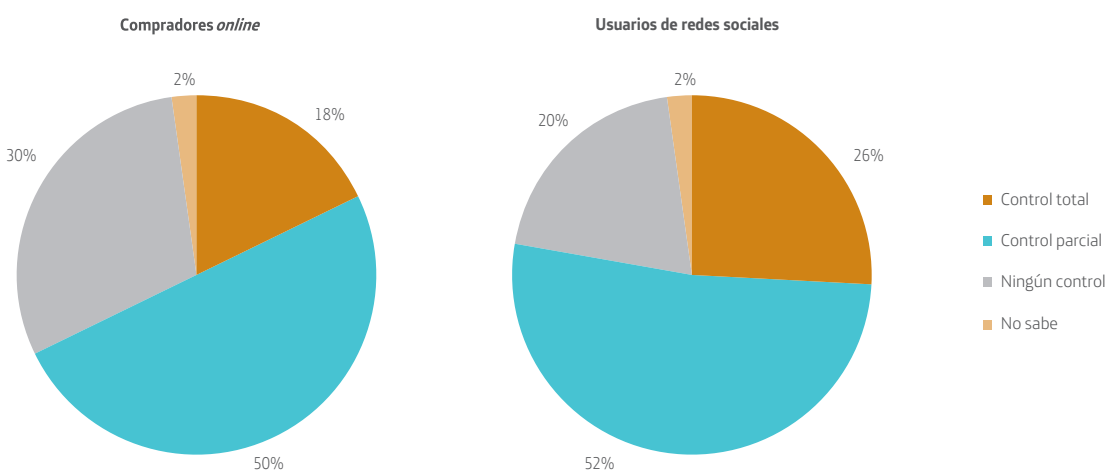
3.8 ¿Quién tiene que controlar la información?

El control sobre la información que se muestra de los usuarios en Internet es otra de las grandes preocupaciones generalizadas.

Respecto a este punto existe una gran división y predomina la sensación de que los usuarios tienen un control parcial sobre sus datos, tanto en el caso de las redes sociales como en el de la compra *online*. En concreto, según el estudio de la UE, el 18 % de las personas que compran *online* sienten que tienen un control completo, el 50 % sienten que tienen un control parcial y el 30 % que no controlan nada.

En el caso de las redes sociales, el 26 % de los europeos cree tener control total sobre la información que comparte (en lo que se refiere a cambios, borrado o corrección de la información), el 52 % cree tener un control parcial y el 20 % siente que no controla nada (figura 17).

Figura 17. Control sobre la información personal que se ha revelado en Internet (UE)



Fuente: European Commission. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. Junio, 2011.

Por otro lado, el 70 % de los usuarios están preocupados por el hecho de que las empresas que han recogido información de un usuario, la puedan utilizar para otros fines distintos de aquellos para los que fue suministrada, y el 74 % piensa que este hecho debe ser aprobado por el usuario al que corresponda, independientemente del uso que se le quiera dar.

Además, la inmensa mayoría, el 75 %, piensa que la información que las empresas poseen de los usuarios debe borrarse en el mismo momento en que el usuario lo decida. En el caso de que cierta información sea robada, la inmensa mayoría de los usuarios, el 87 %, cree que los afectados deben ser informados sobre dicho hecho. Por estos motivos, existe una gran diversidad de opiniones sobre qué entidad deber ser la encargada de asegurarse de que la información es recogida, almacenada e intercambiada de forma adecuada tanto en las redes sociales como en otros sitios de com-

partición de información. Según este mismo estudio, el 49 % de los europeos opina que debe ser el propio usuario. En España existe una mayor división entre los que opinan que este papel debe desempeñarlo el propio usuario, el 37 %; las aplicaciones de redes sociales y sitios de compartición de información, el 29 %, y los organismos públicos, el 33 %.

No cabe duda de que la gestión de la identidad digital (y de parte de ella) es una tarea complicada dadas las características de ubicuidad que posee la información en el mundo de Internet, sobre todo bajo el paradigma *cloud*. El usuario exige, por tanto, mecanismos para participar en la gestión de la información que le atañe. En este sentido, una medida apoyada por el 64 % de los usuarios es la existencia en las empresas de una persona que realizara la labor de punto de contacto con los usuarios, de manera que fuera el interlocutor ante posibles dudas y problemas. Por otro lado, el 71 % de los ciudadanos está a favor de poder llevarse los datos en el momento que cambia de servicio.

Respecto a que otras entidades puedan tener acceso a la información, existe un cierto consenso en que en el caso de la policía sea aceptable que lo haga en el marco de una investigación concreta (con el 37 %), o en actividades generales para la prevención de delitos (en el 33 %) y bajo la supervisión de un juez en el 26 %.

El grado de sensibilidad de los usuarios hacia la información personal lleva a que más de la cuarta parte (el 28 %) de los usuarios de la UE afirme que estaría dispuesta a pagar por tener acceso a la información que tanto entidades públicas como privadas poseen de ellos. En el caso de España, los usuarios no tienen esta disponibilidad y es el país de la UE que muestra porcentajes más bajos en este aspecto, con tan solo un 8 % de los usuarios dispuestos a pagar por ello.

Capítulo 4

La gestión de la identidad digital

Durante los últimos años la huella digital de las personas ha ido creciendo exponencialmente y son muchos los agentes que están trabajando para rentabilizar este conocimiento. Así pues, es razonable que en este escenario crezca la preocupación de las personas por conocer hasta qué punto se están recogiendo datos sobre ellas, quién los usa y cómo.

No hay nada nuevo en el uso de la información del consumidor como producto. La radio, la televisión, las revistas y los periódicos hace tiempo que utilizan la audiencia para atraer anunciantes. Durante años, el marketing directo y las empresas de catálogos han puesto a la venta teléfonos y listas de direcciones. La diferencia es que hoy en día el volumen de información es mucho mayor y que las nuevas tecnologías permiten conocer información que hasta ahora no era posible. A medida que hay más usuarios *online* y que estos renuncian a la privacidad a cambio de conexiones sociales, es más sencillo conseguir más datos. De hecho, según una reciente encuesta,[30] un 34 % de los usuarios de Facebook compartían su fecha de nacimiento completa *online*, un 21 % compartían fotos y los nombres de los hijos, y cerca de uno de cada cinco no se molestaba en usar el control de privacidad de Facebook.

Se está evolucionando desde el concepto de «propiedad sobre los datos» al concepto de «derechos sobre los datos».

La personalización es algo que el consumidor espera y está dispuesto a renunciar a parte de su privacidad por ello. De hecho, en la actualidad existe ya un gran ecosistema de empresas que capturan, agregan, controlan y distribuyen esos datos.

Durante muchos años todo dato sobre una persona tenía un propietario. En la actualidad, el uso generalizado de las nuevas tecnologías ha hecho que esto deje de ser así ya que no se puede asociar una definición de propiedad a información digital que ha sido creada por múltiples partes y que es gestionada, replicada o compartida por otras.

En este contexto, se está evolucionando desde el concepto de «propiedad sobre los datos» al concepto de «derechos sobre los datos», por lo que cualquier modelo de gestión de la identidad digital habrá de tener en cuenta este hecho, y tratar de ofrecer valor a todos los agentes involucrados y, en general, dando soporte a un modelo de derechos de datos abierto.

Se define así la gestión de la identidad digital como la convergencia de procesos de negocio y tecnología capaces de proporcionar seguridad, confianza y privacidad mediante la autenticación de usuarios y su autorización de acceso a recursos de información, aplicaciones y sistemas basándose en su identidad.

4.1 Ciclo de vida de la identidad digital

Para entender bien en qué consiste la gestión de la identidad digital conviene describir antes las fases del ciclo de vida de esta: provisión, propagación, uso, mantenimiento y eliminación.

La primera fase del ciclo de vida de la identidad digital es la de creación o provisión en la cual se da de alta toda la información de la persona, ya sea cliente, consumidor o cualquier otro tipo de usua-

30. Centro Nacional de Investigaciones de Consumer Reports. Junio, 2011.

rio. Hay que destacar que en un entorno empresarial esta información se suministra a los sistemas de la empresa, pero que en un entorno más abierto como es Internet esta fase puede estar distribuida entre múltiples sistemas, servicios y aplicaciones en los que se registra el usuario. En esta fase se incluye información estándar, como puede ser el nombre, la ubicación, el *e-mail* y el teléfono, así como propiedades específicas. Esta fase la puede realizar el propio usuario (autocreación) o bien un administrador del sistema en el que se registra la información.

Cualquier modelo de gestión de la identidad digital deberá ofrecer valor a todos los agentes involucrados dando soporte a un modelo de derechos de datos abierto.

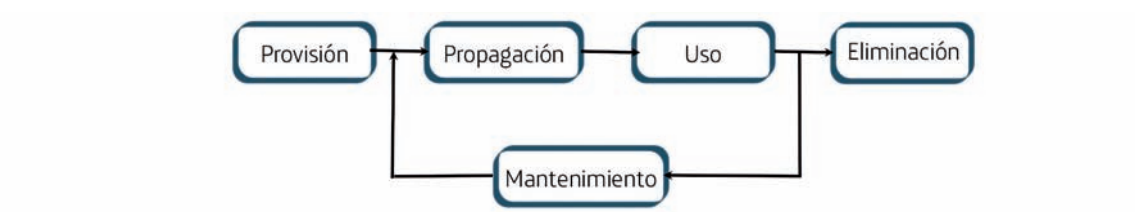
En una segunda fase será preciso propagar el registro de la identidad digital a otros sistemas que así lo necesiten, y para que sea efectiva la propagación debe realizarse de forma fiable tras cualquier modificación. Esta fase del ciclo implica una parte importante de la propia gestión de la identidad digital, que se comenta en más detalle en un apartado posterior.

Una tercera fase sería la de uso. Una vez creada y propagada, la identidad es utilizada por varios sistemas y agentes. El uso de ésta abarca funciones tan sencillas como consultar la identidad para, posteriormente, autenticar y autorizar acciones de los usuarios en los diversos recursos, o acciones más complicadas que implican el acceso a ciertas funcionalidades o la realización de transacciones, etc.

La fase de mantenimiento consiste en la modificación de datos, propiedades, etc., de la identidad que posteriormente habrán de propagarse por el resto de sistemas.

Finalmente, el ciclo de vida se completa con la fase de eliminación de la identidad digital. Se trata de borrar todos los datos de los sistemas (figura 18).

Figura 18. Ciclo de vida de la identidad digital



Por lo tanto, a la hora de diseñar la arquitectura de un sistema gestor de identidad y una infraestructura de identidad digital es fundamental planificar cada fase del ciclo de vida de la identidad de manera que sea posible ofrecer el soporte adecuado.

4.2 Elementos que hay que gestionar en la identidad digital

Se define gestión de la identidad digital como las reglas, los estándares y los procesos mediante los cuales las personas y las empresas gestionan, usan y comparten los datos personales y las identidades de otras personas y empresas.

Tal y como se ha descrito a lo largo de este documento, los usuarios están cada vez más preocupados por los datos que las organizaciones y empresas tienen sobre ellos. La clave para gestionar la

identidad digital consiste, por lo tanto, en ofrecerles control y transparencia sobre sus datos y la capacidad para que la gestionen de manera efectiva.

Bajo esta perspectiva es necesario tratar cinco aspectos: la privacidad de los datos, la seguridad con la que se trata la información personal, la transparencia sobre la información que las empresas y las organizaciones tienen de los usuarios, la portabilidad de la información, y la economía de los datos. A continuación se detalla cada uno de ellos.

4.2.1 Privacidad de los datos

Hasta ahora, los consumidores han estado a merced de las organizaciones. En Estados Unidos, por ejemplo, muchas de las políticas de privacidad de las empresas han estado basadas en los principios de la Comisión Federal de Comercio (FTC)[31], pero se trataba solo de recomendaciones por lo que las empresas podían actuar de la manera que consideraran en lo que a la gestión de los datos de las personas se refiere. En este entorno, el usuario que no estaba de acuerdo con las actuaciones de las empresas solo podía cortar relaciones con esta y aun así no estaba seguro de que todos sus datos se habían borrado de los repositorios.

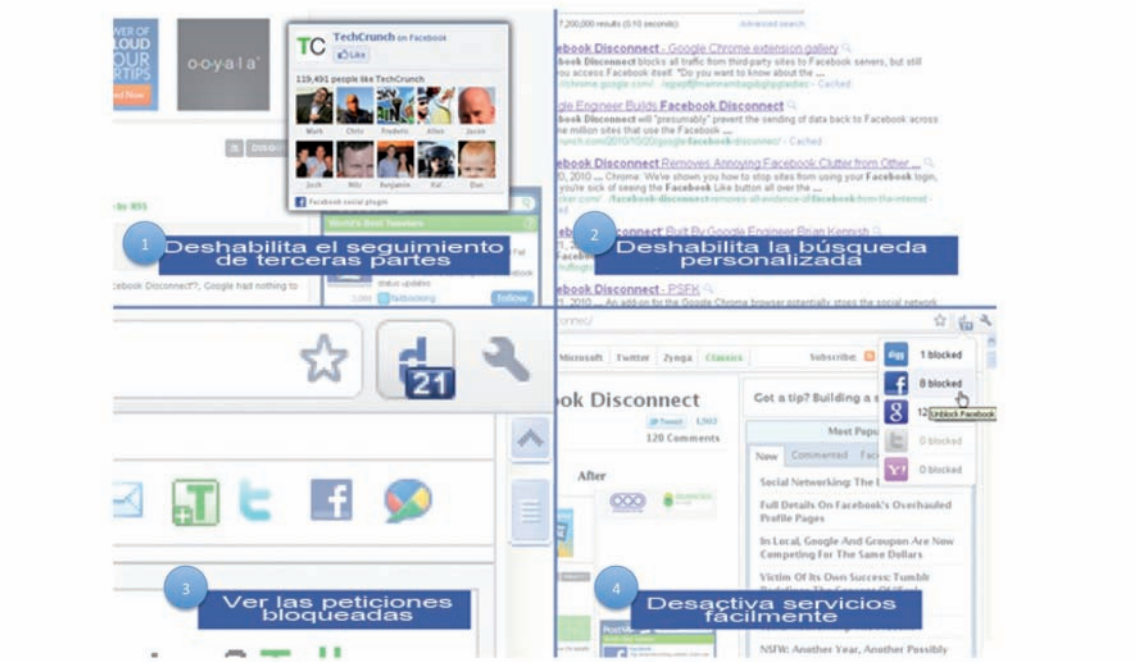
En el nuevo entorno, los ciudadanos esperan políticas que obliguen a las compañías a almacenar únicamente los datos sobre ellos que sean estrictamente necesarios y protegerlos de manera eficaz. Por lo tanto, las organizaciones precisan proveer más control granular sobre los datos. Además, los mercados necesitan cambiar su mentalidad hacia los datos de los usuarios y su privacidad, y trabajar con todas las partes interesadas para aclarar las políticas existentes.

Se trata de respetar los datos personales y explicar a las personas por qué se puede confiar en la empresa u organización que los alberga. En este sentido, es necesario un uso responsable de la información que compone la identidad digital, al mismo tiempo que se respeta al individuo. Se trata de que el usuario pueda decidir qué aspectos de la identidad digital se hacen públicos y qué se comparte, pero también de controlar lo que se sabe de él y de cómo se manejan los datos por parte de las empresas, los organismos y las instituciones.

En esta línea, hay empresas como Disconnect que trabajan para proteger la privacidad de los datos de las personas, en concreto, en relación con los datos de navegación. Los *widgets* incrustados en las páginas web, que permiten a los usuarios enlazar contenido en sus perfiles, permiten también a las redes sociales conocer qué webs visitan sus usuarios, incluso sin que el internauta pulse en el *widget*. Disconnect es una herramienta para el navegador que permite bloquear *widgets* de terceras partes como Digg, Facebook, Google, Twitter y Yahoo (figura 19).

31. Federal Trade Commission.

Figura 19. Disconnect



4.2.2 Seguridad de los datos

Durante años, la seguridad estaba basada en la protección de los datos frente a virus, *malware* y niveles de encriptación y, por lo tanto, era vista únicamente como un problema de tecnologías de la información. Sin embargo, la dimensión seguridad abarca más aspectos. Se trata de gestionar de manera adecuada el uso de los datos, definiendo políticas de gobernanza a nivel global que precisen claramente quién puede acceder a qué información.

Comprometerse en proporcionar seguridad a los datos es fundamental para ganarse la confianza de los usuarios y, por lo tanto, es un aspecto esencial en la gestión de la identidad digital.

Existen muchos mecanismos y niveles de seguridad. Desde el punto de vista de la identificación y el acceso, se cuenta con las contraseñas de acceso, el uso del DNI electrónico, las tarjetas de identificación electrónica, la huella dactilar digitalizada, la identificación biométrica, etc. Muchos de estos sistemas no han tenido el éxito previsto por la necesidad de despliegue de lectores o por la escasa usabilidad que ofrecen. Más allá, existen mecanismos avanzados[32] que permiten, por ejemplo, detectar el fraude en el acceso a ciertos servicios, como los e-financieros (suplantación de personalidad) para lo que se basan en el comportamiento de la persona[33] que accede (en este caso, el comportamiento es parte de su identidad digital).

32. El producto RSA eFraud se basa en esta idea.
33. Navegador usado, lugar desde el que se conecta, país, dirección IP empleada, horario, etc.

4.2.3 Transparencia de los datos

El usuario quiere saber qué información tienen de él y qué hacen con ella. Dar cierto control y ofrecer transparencia sobre los datos incrementa la confianza en el servicio y en los agentes que lo proveen. El objetivo no es abrumar al usuario ni cargarle con tareas extra, sino darle la oportunidad, en el caso de que lo requiera, de corregir, actualizar y borrar sus datos cuando lo desee. Se trata de ofrecer valor a cambio del servicio y en este sentido tiene que orientarse esta transparencia.

Las empresas que sepan comunicar mejor y de manera efectiva el valor de los datos a los usuarios serán las que se beneficien de un conjunto de datos mejor, verificado y completo y, por lo tanto, las que mejor se desenvolverán en el ecosistema competitivo.

4.2.4 Portabilidad de los datos

La portabilidad engloba dos ideas: por un lado, que los datos de los usuarios pueden ser estandarizados de manera que se pueden usar en muchas partes y por otro, que los datos portados están adjuntos a la identidad verificada de la persona.

La portabilidad no ha sido un concepto tradicionalmente asociado con los datos personales porque no había sido necesario. En la actualidad, los clientes no entienden por qué tienen que repetir sus datos personales a diferentes grupos dentro de la misma organización. En este sentido, la adopción de los estándares de autorización y *single sign-on* es la solución para que los datos de los usuarios puedan ser usados en diferentes lugares sin tener que repetirlos.

La portabilidad es un aspecto que beneficia tanto al consumidor como a las empresas ya que no solo influye en la comodidad del usuario a la hora de gestionar su información, sino que desde el punto de vista de los negocios contribuye a la eficiencia. En el caso de PayPal, por ejemplo, su modelo permite portar datos de manera fiable, lo que agiliza los procesos de compraventa electrónica.

4.2.5 Economía de los datos

El futuro de la economía de los datos de los usuarios es incierto, pero es evidente que los ciudadanos desempeñarán un rol importante en él. Actualmente, el modelo tiene unos claros ganadores: los agregadores y recolectores de información, los departamentos de marketing y los agentes de mercado. Hoy día, el ecosistema funciona como un mercado B2B en el que empresas que se dedican a la recopilación de datos sobre usuarios, los modelan y revenden a publicistas y diferentes tipos de empresas que los usan para presentar una oferta más segmentada a las necesidades de los usuarios. Sin embargo, estos modelos se están transformando precisamente por la capacidad actual de las organizaciones de registrar información sobre el usuario de manera sencilla. En este nuevo ecosistema las organizaciones tienen que redefinir qué datos son valiosos. No está claro que los consumidores vayan a tener una remuneración económica por compartir sus datos, pero sí que entrarán en juego las nociones de valor.

Entre las ofertas que los usuarios pueden recibir en contraprestación por la compartición de sus datos se encuentra la recepción de contenidos centrados y relevantes para ellos, así como des-

cuentos y ofertas especiales. Otro aporte de valor podrá ser mediante un sistema en el que los consumidores acumulen puntos a lo largo de ecosistemas cerrados de servicios y proveedores que quieran retener al máximo el acceso a los datos de consumidor. Otro ejemplo de valor extra será la dotación de una oferta personalizada.

Los usuarios tienen que percibir así un valor extra al dar sus datos y como consecuencia confiarán en las empresas que los gestionen. Si entienden bien las causas, las consecuencias y las compensaciones sociales por permitir el uso de los datos, el éxito del modelo estará asegurado.

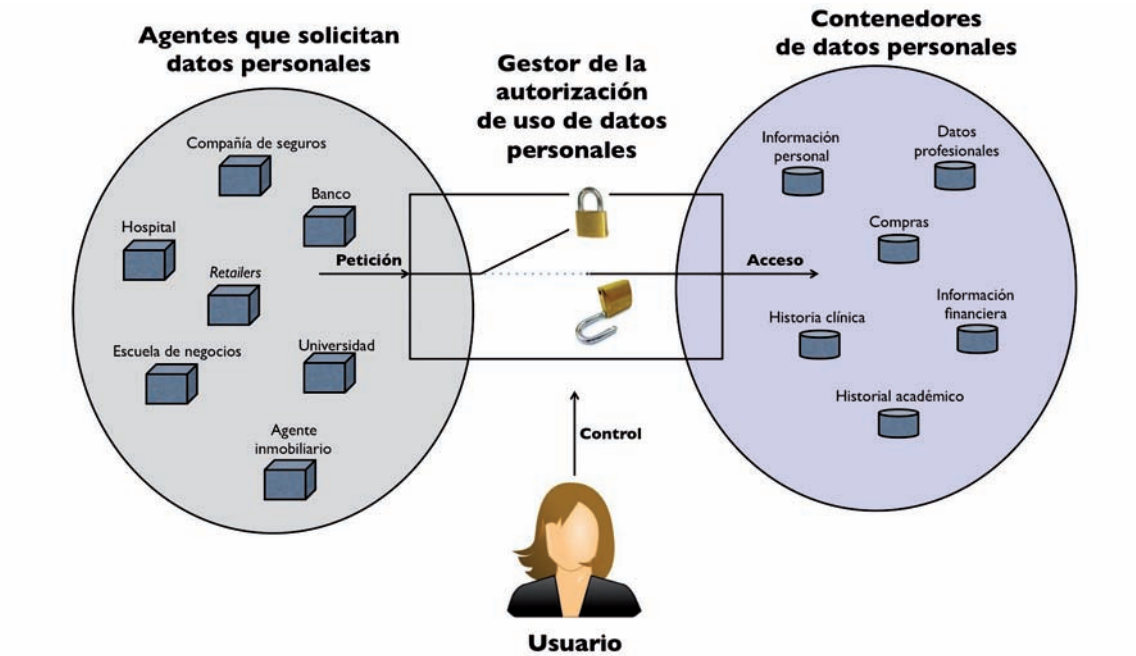
4.3 Componentes de un gestor de identidad digital

Tal y como se ha descrito, la gestión de la identidad digital tiene que ver, por un lado, con ofrecer soporte a su ciclo de vida, y por otro, con ofrecer apoyo a la gestión de los cinco elementos que intervienen en ella: la privacidad, la seguridad, la transparencia, la portabilidad y la economía de los datos.

Hay múltiples modelos posibles para gestionar la identidad digital. Por un lado, estarían los modelos extremos: aquellos en los que existe una base de datos gestionada por la Administración Pública en la que se recoge información sobre la persona y que se encuentra regulada por leyes que controlan el acceso y la verificación de los datos. En el otro extremo estarían modelos que promoverían el mantenimiento personal de todos los datos personales, incluidas las transacciones. No obstante, se entiende que el modelo más probable es uno que combine el de agentes que posean parte de información sobre las personas y el de gestores que autoricen el acceso a dichos datos.

De manera genérica, los componentes de un gestor de identidad serían, por lo tanto: los contenedores de los datos de los usuarios, los agentes que solicitan los datos personales, los gestores de autorización de uso de los datos personales y el propio usuario. Además, podría incluirse la figura de bróker, que actuaría como intermediario (figura 20).

Figura 20. Componentes de un gestor de identidad digital



Fuente: elaboración propia a partir de Forrester.

4.3.1 Contenedores de datos personales

Se trata de los agentes que almacenan los datos personales. Cada uno servirá para diferentes propósitos pero todos estarán gobernados por un conjunto de protocolos comunes. Existen dos modelos de contenedores: por un lado, los que almacenan información sin ánimo de lucro y que normalmente no requieren una actualización frecuente de datos o una gestión granular de esta, y que se rigen por guías regulatorias; y por otro, los agentes comerciales, que generalmente son proveedores de servicios y que sí que se lucran por verificar la identidad, gestionar la reputación o por acceder a los datos de los clientes.

Los repositorios o contenedores pueden almacenar datos de diferentes tipos, ya sean relativos a compras, financieros, profesionales, del ámbito educativo o de salud, etc.

4.3.2 Agentes que solicitan los datos personales

Se trata de terceras empresas, organizaciones o terceras personas que solicitan el acceso a los datos que forman parte de la identidad digital de la persona. Los solicitantes de información pueden ser bancos, empresas de seguros, médicos, comercios, etc.

4.3.3 Gestor de la autorización de uso de los datos personales

Consiste en el rol que facilita el acceso a los datos almacenados en los diferentes contenedores. Puede que este rol en algunos casos forme parte de los contenedores de datos, en otros casos puede ser el propio usuario el que gestione de manera manual el acceso a sus propios datos.

En cualquier caso, se facilita una herramienta que permita a los usuarios actualizar, gestionar y validar datos. Además, ha de servir como mecanismo para que los consumidores aprueben las peticiones de datos y los compartan de manera proactiva con industrias, marcas, proveedores de servicios y otros usuarios.

4.3.4 El usuario en la gestión de sus datos

El usuario es una pieza clave de todo este ecosistema y, tal y como se ha descrito, estará dispuesto a compartir datos de manera explícita a cambio de valor, ya sea como mejores experiencias, comodidad u ofertas. Es evidente, por lo tanto, que el usuario desempeña un rol central en lo que a la gestión de su identidad digital se refiere.

Dado el interés que el acceso a los datos personales está levantando entre los usuarios, son muchas las empresas en el campo de Internet y los sistemas de información que se plantean incluir opciones para que los usuarios puedan controlar la información que poseen relativa a ellos. Por ejemplo, Facebook ha cambiado la configuración de seguridad para permitir un mejor control respecto a quién puede acceder y a qué información accede. En este sentido, el operador móvil O2 ha desarrollado un sistema que permite al usuario un control exhaustivo de la información que el operador posee sobre él, que puede variar desde información relativa a localización y preferencias, hasta el historial de navegación. Los clientes pueden así seleccionar el nivel de aceptación para que esta información pueda ser usada para ofrecerles ofertas de servicios personalizadas y una vez seleccionado este nivel se puedan así realizar variaciones tanto al alza como a la baja en la privacidad deseada. Este sistema muestra a los usuarios qué información posee sobre ellos y de qué forma puede ser utilizada, lo que permite al usuario una mayor involucración en la gestión de sus datos mediante una especie de cuadro de mando.

4.3.5 Nuevos roles en la gestión de la identidad digital: el bróker

Dada la proliferación de sistemas que se alimentan de información de los usuarios, en la actualidad es difícil hacer un seguimiento de dicha información y de qué forma se mueve entre diferentes entidades. Además, la variedad de acuerdos de servicio en las diferentes aplicaciones hace que sea difícil para el usuario poder decidir su planteamiento con respecto a la privacidad de sus datos, o tener una política personal a este respecto.

Por este motivo, han surgido servicios que se dedican a actuar como brókers de los datos de los usuarios. Es decir, que actúan de intermediarios entre los usuarios y las empresas finales que utilizan la información, tratando de esta manera de conseguir el mayor beneficio posible para ambas partes.

En la actualidad todavía estas aplicaciones tienen dificultades para llevar a cabo su propósito ya que los procesos de las empresas de este sector no están preparados en muchos casos para

enlazarse con este tipo de aplicaciones. No obstante, a pesar de estas dificultades, existen aplicaciones que aprovechan este espacio para desarrollar su actividad de gestión de los datos de los usuarios.

Un ejemplo de este rol es el de la empresa Allow,[34] que tiene el objetivo de convertirse en bróker de los datos de los usuarios. Este servicio utiliza unas medidas estrictas de control de privacidad de tal forma que el usuario puede controlar en todo momento qué tipo de información puede ser pública y deja en manos de la aplicación todos los mecanismos de negociación de sus datos con terceros. Entre las ventajas que este modelo implica para el usuario se encuentran las de limitar la intrusión de cientos de mensajes hacia el usuario en diferentes modos, como spam, SMS, llamadas no deseadas, correo publicitario..., el de conseguir que aquellas ofertas o información que se adapten a los gustos del usuario lleguen finalmente a él y, por último, ofrecen al usuario parte del beneficio que terceras empresas puedan dar por sus datos, frente a la política actual de ventas de datos sin ningún beneficio palpable para el usuario (figura 21).

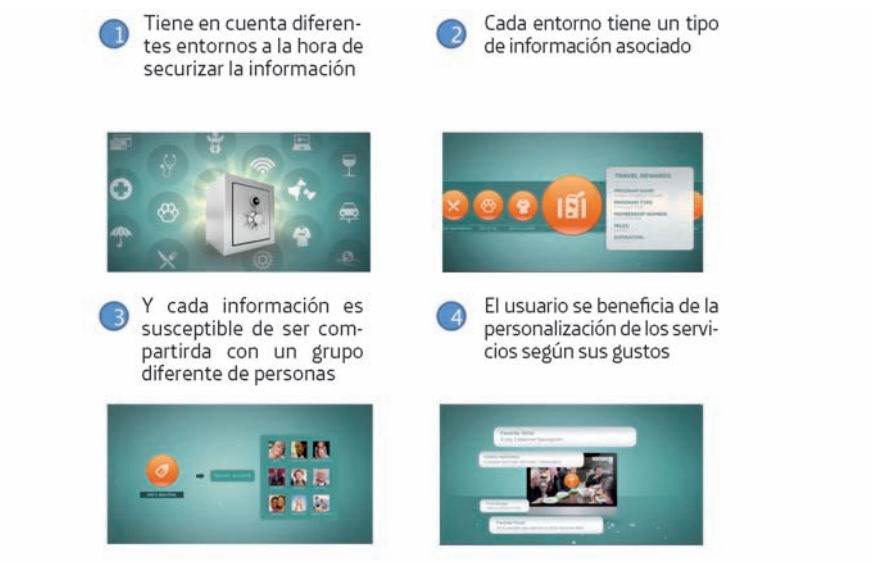
Figura 21. Modelo de servicio de Allow

Otro ejemplo de bróker es Personal.com,[35] un servicio que funciona también como intermediario de datos, y que se orienta a la gestión de la diferente información de usuario que se puede compartir con otras personas o entidades en los distintos ámbitos de la vida. Su idea se basa en la diferenciación de los distintos perfiles que un usuario tiene en su vida cotidiana. De esta forma, un usuario puede compartir información de un marcado carácter profesional con todo el círculo de personas relacionadas con su trabajo y, por otra parte, datos relativos a sus hijos con la familia y la persona que los cuida. El beneficio obtenido tiene que ver con una correcta gestión de la información con terceras personas, así como el hecho de diferenciar perfiles para así personalizar servicios.

34. http://i-allow.com/
35. http://www.personal.com/

Un ejemplo de aplicación se muestra en la figura 22, y consiste en ofrecer ofertas al cliente en función del conocimiento que se tiene de los gustos del consumidor. Esta personalización puede llegar a tener una gran importancia, como en el caso de información referida a la salud: alergias, enfermedades... que puede llegar a ser útil si se tienen que recibir servicios médicos, y sobre todo en emergencias como accidentes en las que es necesario llevar a cabo acciones rápidas.

Figura 22. Modelo de servicio de Personal.com

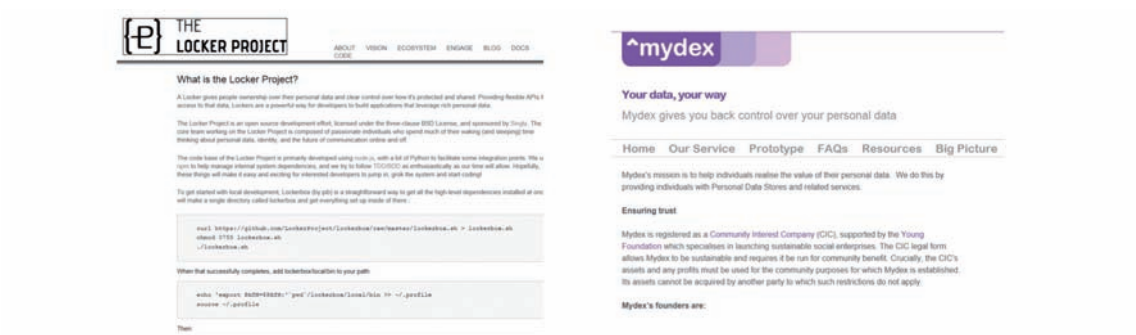


Dentro de esta actividad de brókers de información, algunas empresas han optado por centrarse en un nicho del mercado. Este es el caso de Mint, que tiene como objetivo ayudar al usuario a gestionar sus finanzas personales y a obtener el mayor beneficio de ello. Para conseguirlo, la empresa tiene que vencer las reticencias iniciales de que el usuario confíe en ella y suministre datos tan confidenciales como los números de sus cuentas bancarias, de las tarjetas y las claves de uso. Sin embargo, en la actualidad el servicio cuenta con 5 millones de usuarios, lo que indica que, a pesar de la barrera inicial de revelar información personal, si el usuario recibe nuevos servicios o siente mejoras en los que recibe, suele aceptar el revelar dicha información. En el caso de este servicio, algunas de las mejoras que consigue el usuario son la integración en una cuenta de toda la información personal que procede de diferentes cuentas, bancos, y análisis integrado de los conceptos de gasto, las recomendaciones de productos más rentables según el perfil del usuario y de rebajas, y las alertas financieras: situaciones anómalas, previsiones de pagos, equivocaciones en comisiones, inactividad poco corriente de las tarjetas, etc. (figura 23).

Figura 23. Modelo de servicio de Mint

También empiezan a aparecer modelos de gestores de datos que tienen una finalidad no económica. Se trata, sobre todo, de modelos que tienen validez para tipos de datos que no requieren una gestión frecuente y granular, y circunscritos a ámbitos muy concretos, por ejemplo, en el entorno hospitalario. Algunos ejemplos son The Locker Project y Mydex Data Services (figura 24).

Figura 24. *Brókers* de datos de organizaciones sin ánimo de lucro



Fuente: www.lockerproject.org y www.mydex.org

Todas estas herramientas analizadas están orientadas a ofrecer un servicio a los usuarios en el que destaca como beneficio la compartición de datos con el fin de conseguir servicios mejorados o beneficios económicos.

En el caso de la aplicación i-behavior, el enfoque es diferente. En este caso, los clientes son empresas que desean contar con datos de usuarios correctamente segmentados con la intención de mejorar el impacto de campañas comerciales. Este planteamiento supone un beneficio tanto para las empresas, que al utilizar dichos servicios conseguirán mejorar su eficiencia en las campañas, como para los usuarios, que de esta forma podrán beneficiarse de acciones comerciales adaptadas a su perfil. i-behavior tiene una marcada orientación hacia las compañías, su modelo de negocio se basa en ofrecer información de calidad sobre usuarios a las empresas y para ello cuenta con una amplia base de datos de clientes que puede ser utilizada para acciones comerciales. Su potencial se basa en una completa base de datos de usuarios con gran nivel de segmentación, que permite hacer ofertas personalizadas teniendo en cuenta la situación personal de los usuarios, e incluso ofrecer cupones de descuento basados en la localización (figura 25).

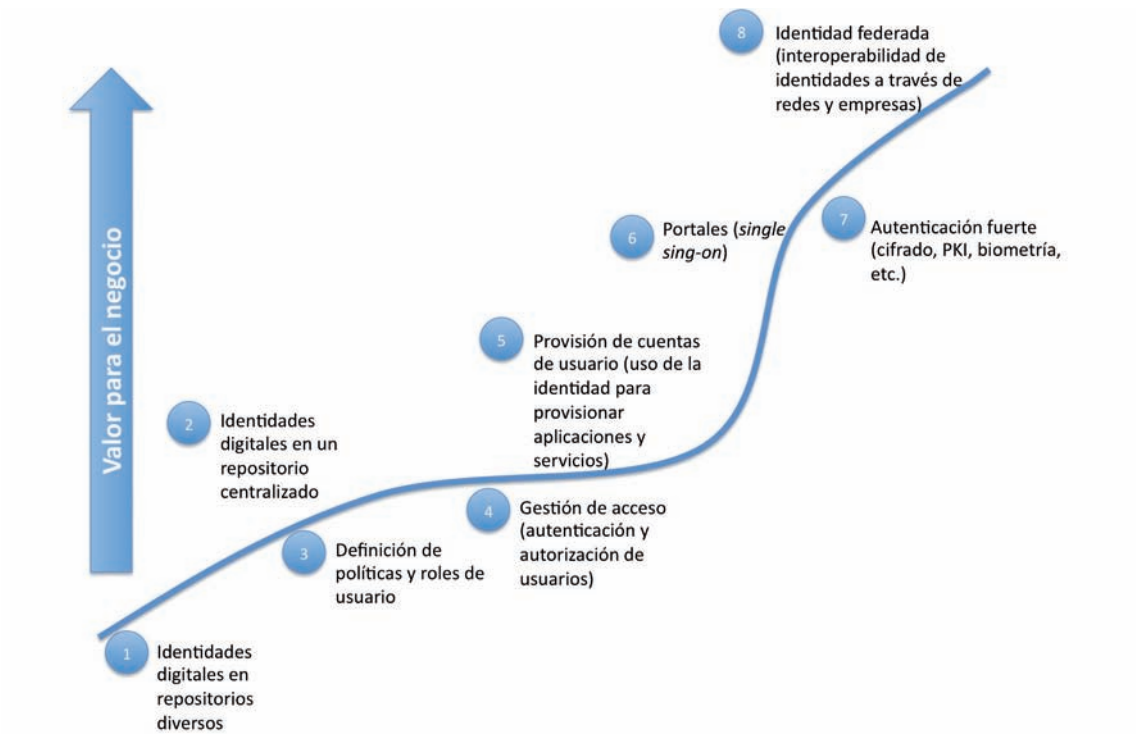
Figura 25. Funcionamiento de i-behavior

4.4 Hoja de ruta de la gestión de la identidad digital

A modo de resumen, cabe señalar cómo ha ido evolucionando la gestión de la identidad digital. Desde una gestión aislada en islas de sistemas o aplicaciones hasta una telaraña de repositorios con una gran cantidad de información sobre la identidad digital redundante o incluso inconsistente. En esta hoja de ruta se pone de manifiesto la importancia de tener un modelo de gestión de la identidad unificado ya que añadir tecnología por tecnología no sirve para poner orden en la telaraña.

Es interesante entender que la gestión de la identidad digital es un término que apareció en el ámbito de la empresa y que tenía que ver con los sistemas de esta, sus políticas de seguridad, procedimientos, procesos de negocio y arquitectura, y que en la actualidad se ha convertido en una realidad más amplia, que abarca más allá del ámbito de los sistemas corporativos como tales y cuyo máximo valor se alcanza en la gestión de la identidad de manera federada, de modo que exista interoperabilidad de identidades a través de redes, empresas, organizaciones, etc. (figura 26).

Figura 26. Hoja de ruta de la identidad digital



Fuente: Elaboración propia.

Capítulo 5

El valor económico y social de la identidad digital

La identidad se define como toda la serie de rasgos que identifican a una persona. Estos rasgos pueden ser de muchos tipos, desde físicos hasta características demográficas, capacidades o comportamientos.

El concepto de identidad, tal y como se ha descrito a lo largo de este informe, desempeña un papel fundamental en todo tipo de relaciones. De hecho, las relaciones personales entre amigos o grupos sociales tienen como aspecto fundamental para poder desarrollarse la capacidad de identificación rápida y sin ambigüedades de los miembros que componen el grupo. Sin embargo, a medida que el grupo de personas es más amplio, los atributos físicos no son suficientes y es necesario algún tipo de documento o certificación para acreditar la identidad de las personas. Un ejemplo de ello se puede ver en las relaciones con la Administración Pública o con entidades como los bancos. Así, en una sucursal bancaria, es muy probable que el cajero que se encuentra en dicho momento despachando no conozca al usuario, que deberá presentar algún documento acreditativo como el DNI para que puedan tener lugar las transacciones de forma segura (figura 27).

Figura 27. El avance en los medios de identificación impulsa la economía

Fuente: Elaboración propia.

Desde el punto de vista económico, el aseguramiento de la identidad tiene un valor fundamental, ya que las actividades económicas requieren un elevado grado de confianza y seguridad. Es, por tanto, fundamental para que la economía se desarrolle de una forma eficiente la existencia de una serie de garantías formales que permitan asegurar que las actividades se desarrollan de una forma adecuada y no existe ningún tipo de fraude. Hasta ahora todos estos sistemas orientados a garantizar la identidad de los usuarios han supuesto una gran cantidad de trámites y de recursos, en definitiva, un gasto, en tiempo y dinero, lo que suponía un sobrecoste para toda la actividad económica. De hecho, la excesiva burocracia supone en sí una traba al desarrollo de la actividad puesto que dificulta todo el proceso asociado a cualquier actividad económica. La digitalización de mucha información y el desarrollo de sistemas informáticos han sido elementos clave en el crecimiento económico de los últimos años. Las empresas se han beneficiado de la posibilidad de realizar transferencias de forma sencilla y segura, y no solo las empresas sino también los propios ciudadanos han aprovechado esta mejora, tanto desde el punto de vista de nuevas capacidades como en la comodidad. Por ejemplo, el hecho de que un usuario pueda sacar dinero de un cajero automático mediante la utilización de una tarjeta que posee un PIN asociado es, sin duda, una función que facilita la gestión económica personal (tabla 3).

Tabla 3. Beneficios que ofrece la identidad digital en la dispensación de dinero desde un cajero automático

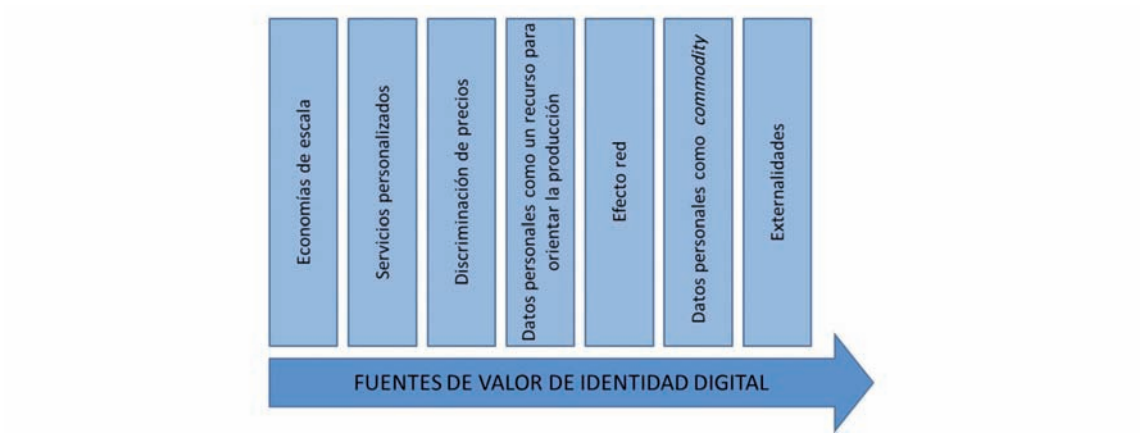
Servicio 7 días x 24 horas	El usuario puede acceder al servicio sin tener que amoldarse a horarios concretos o con las limitaciones de los días laborables
Reducción de costes generales por prestación del servicio	Los cajeros automáticos tienen asociados unos costes de servicio inferiores a los de las personas
Mayor red de puntos desde los que usar el servicio	La red de cajeros automáticos pone a disposición de los usuarios más puntos desde los que poder acceder al servicio de dispensación de dinero

Por lo tanto, la posibilidad de digitalizar los datos y de poseer medios digitales de identificación permite reducir los costes de prestación de los servicios con la consiguiente mejora en la productividad. Este es el aspecto en el que se centraron los cajeros automáticos en Japón en un principio, y los dispositivos expendedores automáticos se encontraban en el interior de las oficinas por lo que se limitaban a reemplazar al cajero. En cambio, en Occidente, el desarrollo se centró en las nuevas ventajas que proporcionaba esta nueva forma de servicio, como son la eliminación de barreras de tiempo y también de espacio a la hora de acceder al servicio, lo que supuso una utilización masiva.

Internet ha supuesto un cambio sin precedentes como medio de comunicación y con el cual se realizan transacciones económicas, permitiendo una ubicuidad casi completa en el acceso, sobre todo desde que Internet móvil ha ido ganando relevancia. Se dispone, por tanto, de una herramienta mucho más potente que cualquier otra que haya existido con anterioridad para realizar transacciones y consultar información. En todo este entorno, la existencia de mecanismos que certifiquen la identidad de las partes que participan adquiere una importancia capital para poder asegurar esta actividad así como para que pueda seguir aumentando en el futuro.

En la figura 28 se detallan los principales beneficios que ofrece Internet basados, en gran medida, en el desarrollo amplio del concepto de identidad digital.

Figura 28. Beneficios del desarrollo amplio del concepto de identidad digital en Internet

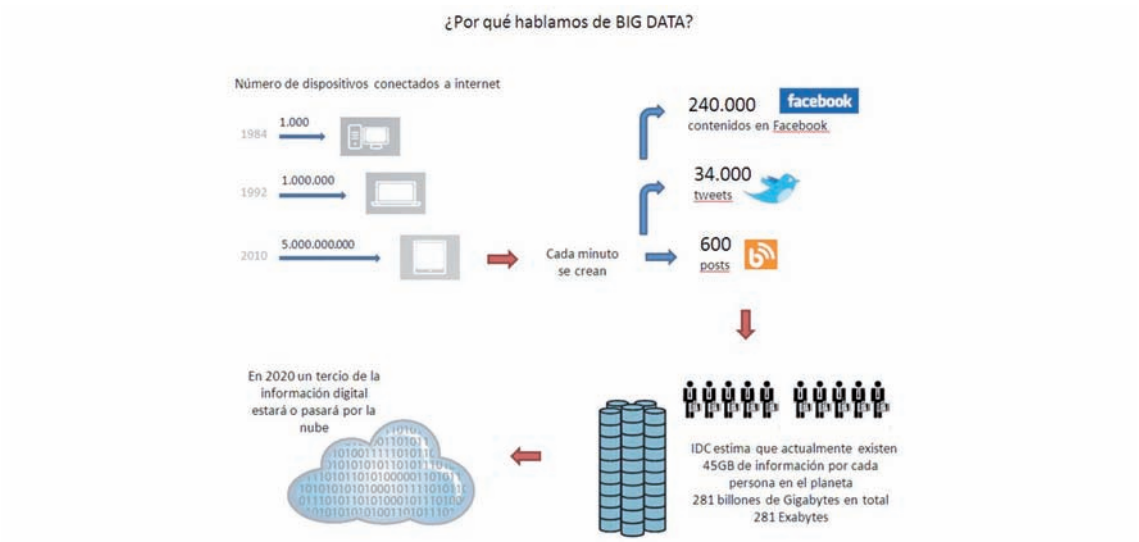


5.1 Economías de escala

La digitalización de grandes cantidades de información, así como el aumento de las capacidades de procesado y las posibilidades de los sistemas de minería de datos que permiten segmentar a los usuarios, suponen una reducción de costes importante como consecuencia precisamente de la escala.

En la actualidad, la huella digital de los usuarios en Internet es muy elevada; está formada por una gran cantidad de datos, muchas veces con carácter desestructurado, y en la que se combina información tanto cualitativa como cuantitativa. Esta información abarca desde comportamientos en las páginas y servicios web, hasta comentarios, votos, compras... realizados por el usuario. Dadas las características de esta gran masa de información, están apareciendo nuevas aproximaciones en el análisis de datos para conseguir sacar el máximo provecho. En este sentido, el término Big Data se está consolidando para describir un nuevo modelo de análisis de grandes volúmenes de información que va a permitir entender cada vez mejor el comportamiento de los clientes (figura 29).

Figura 29. Big Data



Fuente: Elaboración propia.

5.2 Servicios personalizados

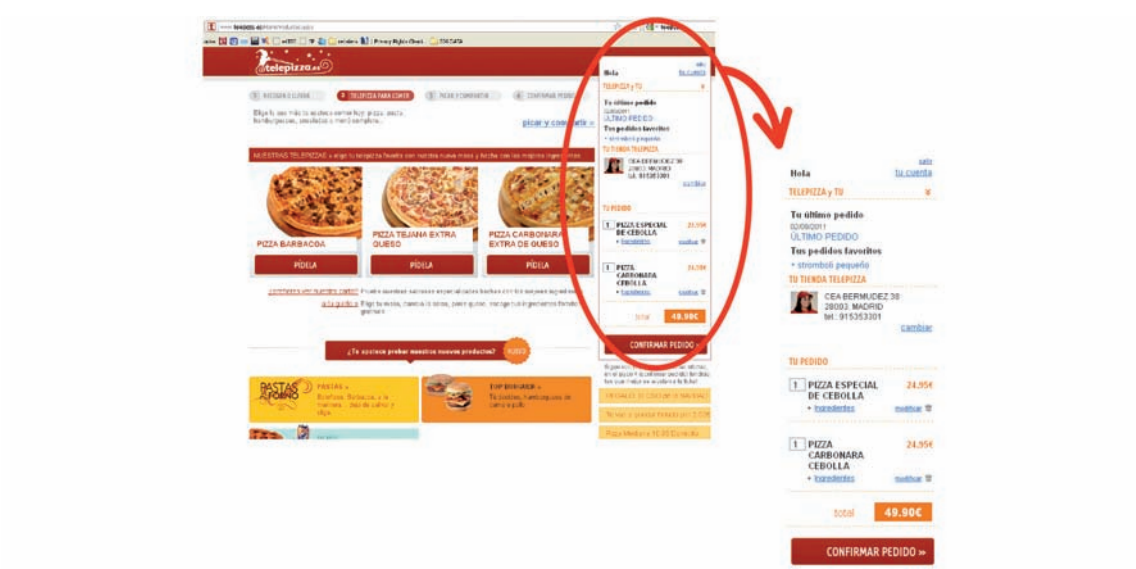
En la actualidad, la personalización es un aspecto cada vez más importante en la comercialización de los productos y servicios. Son habituales las ofertas adaptadas a perfiles de usuarios que tratan de mejorar las posibilidades de éxito de las acciones de venta ya que ofrecen valor tanto para las empresas, como para los usuarios. Sin duda, la información del usuario es clave para configurar estas ofertas y, por lo tanto, para lanzar este tipo de servicios cada vez más demandados (figura 30).

Tal y como se ha detallado a lo largo del informe, los usuarios estarán dispuestos a compartir datos por comodidad y por valor. Así que el marketing evolucionará de la orientación a campañas a una visión más científica que tendrá en cuenta el análisis de los datos de los usuarios basado en su comportamiento. Será un análisis más continuo y fluido, no basado en un único episodio, tareas o en segmentación. Se tendrán que implementar modelos que permitan analizar datos «al vuelo» y con ello plantear una nueva manera de gestionar los datos de los usuarios. En definitiva, quien controle los datos de los usuarios controlará las relaciones comerciales.

Figura 30. Oferta de trabajo personalizada

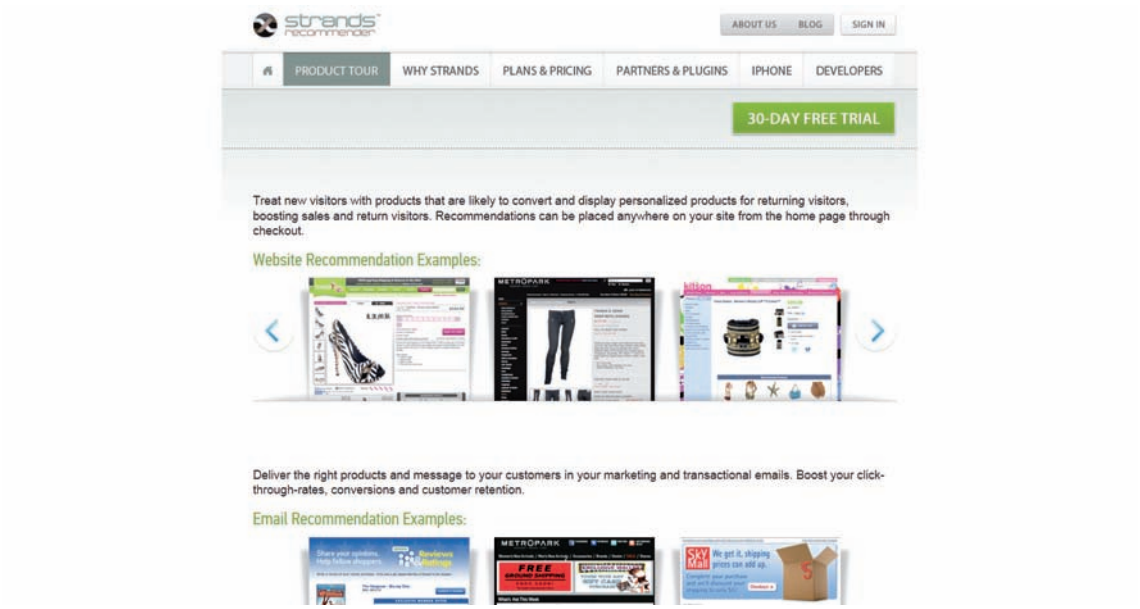
Un ejemplo de empresas que, buscando estas ventajas, han realizado la personalización de servicios *online* es Telepizza. Los datos que recoge Telepizza.es al crear una cuenta y los que almacena en sucesivos pedidos le permiten prestar un servicio personalizado con características como el último pedido realizado, los pedidos favoritos o la tienda asignada (figura 31). Este tipo de servicio facilita la compra al comprador y repercute positivamente en las ventas.

Figura 31. Personalización de servicios en Telepizza.es



La importancia de ofrecer información personalizada para aumentar el ratio de compras de los usuarios ha llevado a la creación de herramientas cuyo objetivo es ofrecer este servicio a terceras empresas. Es el caso de la herramienta Strands Recommender, de Strands Labs, que está enfocada a empresas de tamaño medio que no tienen capacidad de desarrollar su propio sistema, pero que quieran disponer de las ventajas que los recomendadores ofrecen a la hora de personalizar la oferta a los usuarios (figura 32).

Figura 32. Herramienta de personalización de ofertas Strands Recommender



5.3 Discriminación de precios

Este aspecto puede considerarse como una particularización concreta de la personalización, ya que en este caso el precio puede ser considerado como un atributo del producto o servicio.

Para ofrecer productos bajo esta idea, es necesario realizar un análisis de gran cantidad de información del usuario para entender sus gustos y prioridades de compra. De esta forma, se pueden hacer ofertas especiales en precio con la finalidad última de obtener los mayores beneficios posibles. Este tipo de actuaciones ya se realizan en la actualidad en el caso de los usuarios de avión con fines profesionales, que son gravados en mayor medida que los usuarios que corren con sus gastos de manera personal. En general, con un mayor grado de información gracias al concepto de identidad digital sería posible una mayor discriminación y, por lo tanto, se podría dar una oferta más adaptada a los usuarios. En este caso en concreto, podrían diferenciarse tres tipos de discriminación[36]: un primer nivel supondría que las empresas son capaces de estimar la máxima cantidad que un usuario está dispuesto a pagar por un producto o servicio; un segundo nivel supone que los usuarios elijan de forma voluntaria las diferentes combinaciones de precio-cantidad de productos y servicios (por ejemplo, un usuario que a la hora de seleccionar un viaje en avión decida quedarse la noche del sábado o utilizar un viaje en clase turista), y un tercer tipo de discriminación supone la fijación de precios basada en las características de un grupo o en sus comportamientos (entradas de cine para los estudiantes y pensionistas...).

36. Acquisity (2008).

5.4 Datos personales como un recurso para orientar la producción

Los datos personales, así como los historiales de comportamientos, pueden utilizarse como fuente de datos a la hora de diseñar nuevos servicios y productos. Este modelo estaría encuadrado en lo que generalmente se conoce como «innovación abierta» y que supone que los propios usuarios participan de alguna manera en el proceso de ideación de nuevos productos. Estos serían mucho más cercanos a las necesidades del cliente, y con una doble mejora: por una parte, una reducción de costes de desarrollo para las empresas, así como una minimización de las posibilidades de fracaso; desde el punto de vista del usuario, también se vería favorecido ya que podría encontrar productos mejor adaptados a sus necesidades y probablemente a un precio más bajo.

Un ejemplo sería Lay's. Esta empresa recoge datos de los usuarios para determinar el diseño del producto. La figura 33 muestra un concurso realizado en 2010 en el que se animaba a los consumidores a proponer diferentes sabores para sus productos.

Figura 33. Lay´s como ejemplo de uso de datos personales para orientar la producción

5.5 Efecto red

El efecto red viene a suponer que el valor de cualquier servicio que tenga las características de red depende del número de elementos que esta tenga. Por ese motivo, cuando los usuarios deciden unirse el valor de dicho servicio aumenta, así como la posible utilidad para ellos.

Un ejemplo de la utilidad del efecto red para que los usuarios puedan conseguir beneficios son las empresas de descuentos que emplean la Red para alcanzar grandes volúmenes de potenciales clientes y así obtener ofertas. Este es un modelo que está teniendo gran auge en el último año y son numerosas las empresas que basan su modelo de negocio en actuar como intermediarios entre empresas de servicios y grandes volúmenes de clientes. Es el caso de GroupOn y Groupalia, entre muchas otras (figura 34).

Figura 34. Modelo de descuentos basados en volumen de clientes

El papel creciente del carácter social y de red de los servicios se produce a todos los niveles y hasta servicios más tradicionales de Internet dan a este concepto un papel creciente. Incluso los buscadores como Google empiezan a tener en cuenta aspectos sociales entre los criterios de búsqueda complementando los criterios tradicionales de SEO (*Search Engine Optimization*), para lo que ha lanzado la aplicación Google Social Search. De esta forma, los propios usuarios influyen con su actividad social en la relevancia de los contenidos.

Pero la importancia del efecto red en el comercio va más allá y son numerosos los negocios que utilizan las redes sociales como plataforma para ejercer su actividad comercial utilizando el valor de lo social.

Zara es un ejemplo de empresa que emplea las redes sociales para generar un efecto de red alrededor de sus productos. Se consigue así la interacción con los usuarios y se crea un diálogo entre ellos sobre los productos que comercializa la empresa (figura 35).

Figura 35. Zara como ejemplo de uso de redes sociales

En otros casos, existen empresas que han creado herramientas que permiten elaborar grafos con las relaciones de los usuarios de un determinado servicio, tal y como se observa en la figura 36. Este tipo de servicios tiene gran importancia en sectores en los que el comportamiento de los usuarios depende en gran medida de su red social de contactos. El conocimiento de esta red permite anticiparse a muchos comportamientos, como por ejemplo el *churn* o cambio de operador. También permite detectar cuáles son los usuarios clave y conocer signos de que un usuario está dando muestras de querer darse de baja. Se consigue así una cierta capacidad de prever comportamientos y de anticiparse a los usuarios con la política comercial.

Figura 36. Herramienta Kxen de análisis de redes de usuarios

Esta opción es especialmente interesante en el caso de los operadores de telecomunicaciones.

5.6 Datos personales como *commodity*

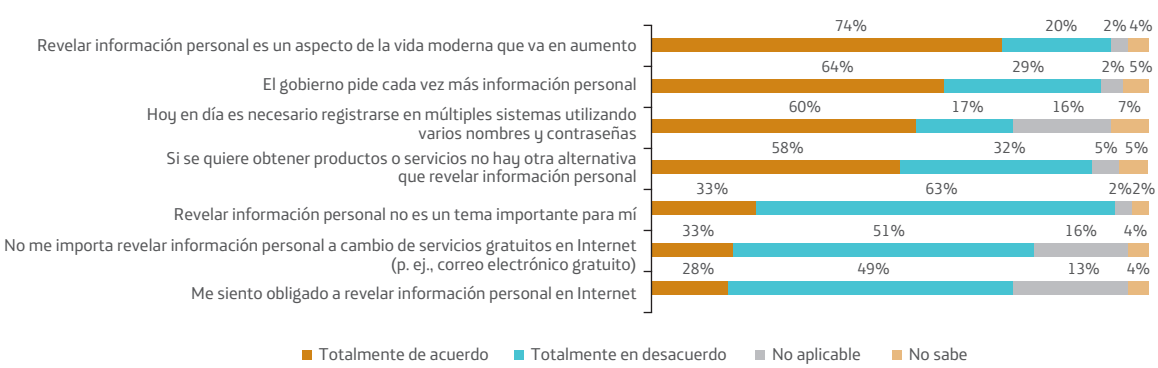
En muchas ocasiones, las entidades que recogen cierta información sobre los ciudadanos no son realmente las que podrían obtener mayor utilidad de su uso. Por este motivo, existe la opción de que una vez aprobada por parte del usuario la transmisión de los datos a otras organizaciones, el usuario pueda obtener beneficios de este proceso. Esta opción requeriría el desarrollo de mecanismos de control de la información.

Los usuarios asumen que la información personal será una parte más del ecosistema de información que hace funcionar la economía.

Sin embargo, los temores de los usuarios a que información que consideran personal pueda fluir de forma no controlada por la Red suponen una reticencia que es necesario gestionar. El desarrollo que se producirá en los próximos años en este ámbito vendrá determinado por la forma en que las alternativas tecnológicas puedan entregar beneficios a los usuarios y evitar al mismo tiempo riesgos de fugas de información.

En la actualidad ya existe una concienciación de los usuarios sobre la necesidad de mostrar información personal a la hora de utilizar ciertos servicios. Por ejemplo, tal y como se observa en la figura 37, el 58 % de los europeos están de acuerdo en que es necesario mostrar información personal a la hora de conseguir productos y servicios (60 % en el caso de los españoles), y lo que es más, el 74 % de la población considera que mostrar información personal es una parte importante de la vida moderna. Esto viene a suponer la aceptación de esta nueva realidad en la que los usuarios asumen que la información personal será una parte más del ecosistema de información que hace funcionar la economía.

Figura 37. Impresiones respecto a la revelación de datos personales en Internet (UE)

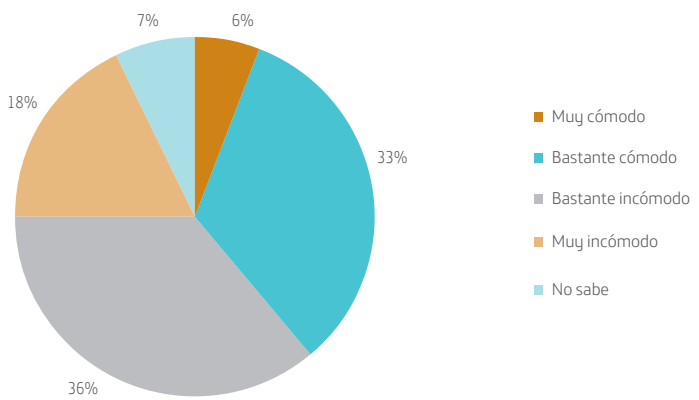


Fuente: Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. European Commission. Junio, 2011.

Las personas son cada vez más conscientes de que existen nuevas reglas de juego que, en muchos casos, implican mostrar información personal. No obstante, el ciudadano también es más exigente y considera que a cambio debería recibir algo que, en ciertos casos, podrían ser servicios gratuitos como una cuenta de correo, una medida que, como se observa en la figura 38, contentaría a una parte importante de los usuarios. En muchos casos, los usuarios no se conforman con esa

compensación y exigen tener acceso a los datos que las entidades tienen de ellos, de su uso (un 70 % muestran preocupación sobre este aspecto), y sobre todo que sean informados cuando haya habido algún imprevisto que pueda suponer un problema de seguridad (87 %). También consideran que debe haber algún tipo de sanción económica (51 %) a las empresas que utilicen inadecuadamente la información, por ejemplo para *spam*, prohibirles su uso en el futuro (40 %) o compensar a las víctimas (39 %).

Figura 38. Grado de comodidad de los usuarios de Internet frente al uso de su actividad *online* para personalizar servicios y contenidos web (UE)



Fuente: Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. European Commission. Junio, 2011.

5.7 Externalidades

Además de los aspectos que se han tratado, es posible encontrar una serie de externalidades, que aunque no sean el objetivo último de la identidad digital, pueden llegar a tener un interés relevante. Estas externalidades se pueden dar en los más diversos ámbitos, como el control de epidemias y el tratamiento personalizado de estas gracias a la información que las administraciones puedan poseer de los ciudadanos, aunque esta sea información agregada y no individualizada. Lo mismo puede suceder en todo tipo de iniciativas públicas sobre infraestructuras, instalaciones, etc. Es decir, disponer de información sobre la identidad digital puede ser de interés en otros ámbitos, en principio, no previstos (figura 39).

Figura 39. Herramienta para estudiar la evolución de la gripe basándose en el comportamiento de la población usando Google

Capítulo 6

Casos de uso de la identidad digital avanzada

El uso enriquecido de la identidad digital ofrece muchas posibilidades a la hora de diseñar nuevos productos y servicios, así como de mejorar los actuales.

Son numerosos los ámbitos en los que pueden aplicarse estas ideas: desde el entorno de servicios de una *Smart City* hasta los procesos de compra *online*, el ámbito sanitario, el entorno educativo, los servicios de ocio, la Administración Pública, los servicios financieros, etc. A continuación se describen en detalle algunas aplicaciones, funcionando o en desarrollo, y que se basan en la utilización de información relacionada con la identidad digital de los usuarios, y se detallan los mecanismos utilizados para mantener la privacidad de estos. Los beneficios repercuten tanto en las empresas como en los usuarios finales, y los retos fundamentales tienen que ver con esta protección de la privacidad.

6.1 Aplicación de la identidad digital al ámbito de los *retailers*

Las empresas del sector comercial hacen grandes esfuerzos para conocer en mayor detalle a sus clientes y de esta forma tener una mayor capacidad para adaptarse a sus necesidades, aumentando las posibilidades de retenerlos y de incrementar así las ventas.

Por este motivo, muchas empresas del sector *retailer,* principalmente las que han nacido con Internet como medio de distribución, realizan grandes esfuerzos en el campo del estudio de la identidad digital de sus clientes. Estos análisis tienen como objetivo lograr una segmentación de los clientes basada en sus comportamientos, más que en variables puramente sociodemográficas. Se trata, por tanto, de conocer sus gustos, sus pautas de conducta, etc., para, de esa manera, ser capaces de adelantarse a sus decisiones y, por ejemplo, poder detectar si un usuario está descontento y quiere cambiar de compañía.

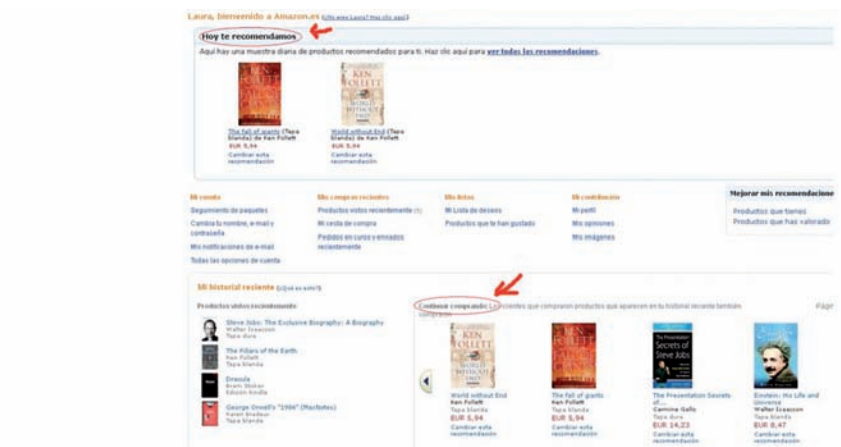
Entre estos sistemas de análisis de los comportamientos de los usuarios, destacan los «recomendadores», que se pueden considerar el paradigma de los sistemas de análisis del comportamiento de los usuarios. Cabe destacar tres modelos claramente diferenciados:

- La recomendación personalizada: Recomendar artículos, basándose para ello en el comportamiento del usuario.
- La recomendación social: Recomendar artículos, basándose para ello en el comportamiento de usuarios similares.
- La recomendación por artículo: Recomendar artículos, basándose en un artículo comprado.

No obstante, la mayoría de los sistemas de recomendación utilizan combinaciones de los tres métodos y tratan de complementar el conocimiento personal que tienen de un usuario concreto con comportamientos de otros que han mostrado pautas de conducta similares. Un ejemplo de empresa pionera en el análisis de los comportamientos de los usuarios es Amazon, que desde el principio basa su negocio en las posibilidades que ofrece Internet, y vio en el estudio de los usuarios una fuente para aumentar sus ingresos y avanzar de esa manera en su intención de «desintermediar» el proceso de venta, al principio de libros y posteriormente de gran cantidad de artículos.

El sistema de Amazon hace un seguimiento personal de la actividad de cada usuario. Entre las opciones que ofrece se encuentra la de recomendar nuevos artículos en función de las compras pasadas y de los comportamientos de los usuarios con características comunes. También muestra el historial reciente de navegación por la página web, así como la posibilidad de que el usuario borre parte de este historial de navegación, dándole el control sobre parte de su información. Tal y como se observa en la figura 40, en caso de que el usuario se registre con su nombre, el sistema personaliza la página de navegación con dicho nombre y agrega toda su actividad, aunque se haya producido desde ordenadores distintos.

Figura 40. Sistema de recomendación de Amazon



En su afán de mantener el contacto con el usuario de una forma más permanente, Amazon ofrece además la posibilidad de enviar información personalizada a cada cliente sobre algunos artículos que pueden resultar de su interés (figura 41).

Figura 41. *E-mail* con promociones personalizadas enviadas por Amazon

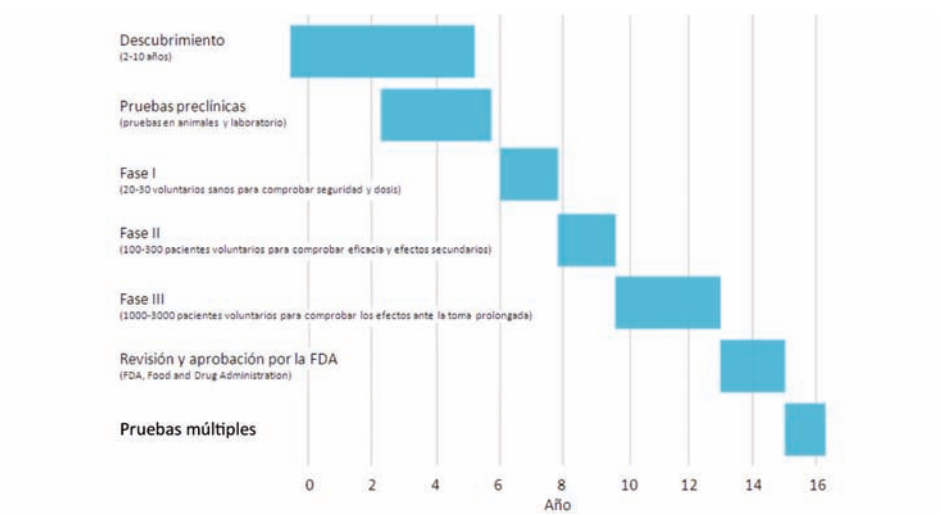
6.2 Aplicación de la identidad digital al ámbito de la investigación farmacéutica

La privacidad de ciertos tipos de datos es un derecho reconocido por las leyes y también valorado por los usuarios. Por este motivo, en muchas ocasiones, no se obtienen todos los beneficios posibles de dicha información. Este es el caso de la información genética, que tiene un carácter muy confidencial para la persona a la que se refiere dicha información pero que podría tener un gran interés desde el punto de vista de la investigación de nuevos productos farmacéuticos. Precisamente un campo en el que estos datos podrían poseer un extraordinario valor es el de la farmacogenética, que trata de estudiar la influencia de los genes en la respuesta de los individuos a las medicinas.

Este es, pues, un claro ejemplo en el que existe un conflicto de intereses entre el derecho a la privacidad de los usuarios y la investigación científica.

Para resolver este tipo de problemas de forma satisfactoria para todas las partes, se ha desarrollado GenoMatch[37], un sistema de gestión de la privacidad para ser usado con datos personales altamente sensibles, como es la información genética, y en entornos muy regulados, como es el farmacéutico. Gracias a este sistema se protege la privacidad de los individuos que participan en los estudios farmacogenéticos. Hay que destacar que los estudios clínicos suelen ser procesos largos, en los que interviene una gran cantidad de usuarios de forma voluntaria y que necesitan de la recolección de múltiples datos clínicos, como las observaciones relativas a los efectos del medicamento y la combinación de estos con la información genética de los participantes para estudiar la influencia de los genes en la efectividad del medicamento y en las reacciones adversas (figura 42).

Figura 42. Fases en el desarrollo de un medicamento



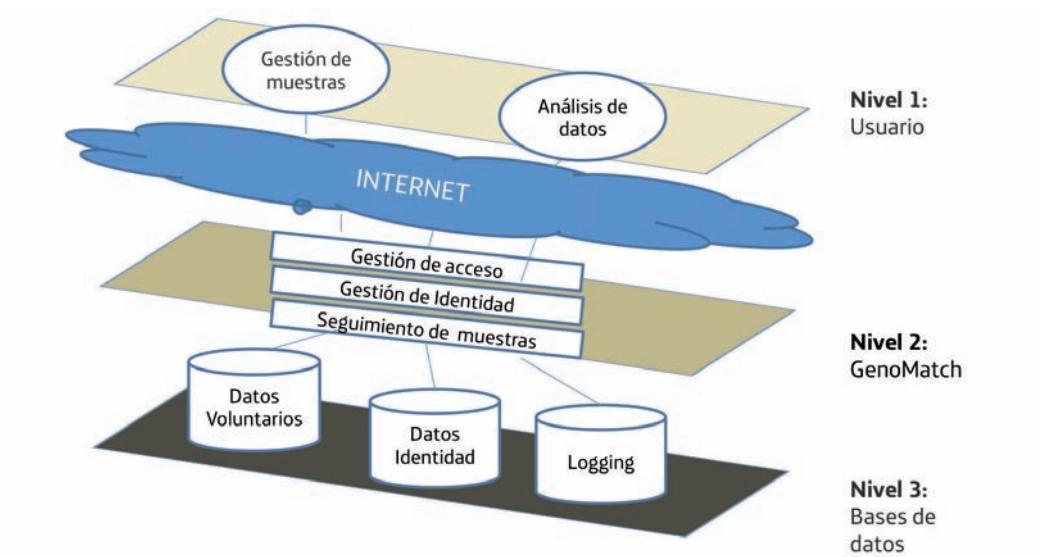
Fuente: Investbio.

37. Desarrollado en el año 2003 como un proyecto cooperativo entre Bayer Schering Pharma AG, investigadores de la universidad de Kiel, y el desarrollador de software Tembit Software GmbH.

GenoMatch gestiona las muestras genéticas en este entorno, con la intención de buscar un equilibrio entre los requisitos de confidencialidad y las necesidades de los investigadores a la hora de establecer vínculos entre toda la información. Para ello, GenoMatch se basa en la implantación de un modelo en tres capas, tal y como se observa en la figura 43, para permitir un equilibrio entre utilización beneficiosa de la identidad digital de los usuarios y las normas de privacidad que aplican a este tipo de información:

- En el nivel 1 se realizan todas las actividades que tienen que ver con el usuario, la gestión de las muestras y el análisis de los datos.
- En el nivel 2 se encuentra el sistema GenoMatch propiamente dicho, cuyas principales actividades son la gestión de acceso de cada agente a los datos que tenga permiso para acceder según su rol, así como la gestión de identidad y el seguimiento de las muestras que permiten conocer su estado en cada momento del proceso.
- En el nivel 3 se encuentran todas las bases de datos.

Figura 43. Modelo GenoMatch para la gestión de identidad



Fuente: Reischl et ál. (2006).

Las tecnologías utilizadas para favorecer la privacidad en este ejemplo están diseñadas para gestionar la identidad con la premisa de que no exista un anonimato completo, según los siguientes requerimientos:

- Las autoridades responsables del licenciamiento de medicamentos requieren el acceso a todos los datos que han sido usados en la investigación previos a la obtención de la licencia.
- Cada participante tiene que tener derecho a terminar su participación en cualquier momento y conseguir que sus datos personales sean permanentemente y fiablemente borrados.

- Los participantes deben ser identificables en los siguientes casos: cuando sus genes revelen información sobre enfermedades (o predisposiciones a enfermedades), de tal forma que sean informados para proteger su salud, y cuando haya interacciones entre genes y medicamentos, lo que puede significar la necesidad de retirar a los usuarios del estudio.

Todo esto viene a significar que los datos de los individuos deben ser trazables e identificables en cada etapa, por lo que se requiere un seudoanonimato, en vez de un anonimato absoluto de los participantes. Para conseguirlo, GenoMatch separa la información en diferentes capas teniendo en cuenta los distintos agentes involucrados en el proceso, mientras que las claves de acceso son custodiadas por una tercera parte que no tiene acceso a la información.

Los beneficios conseguidos con este sistema, que ya utilizan dos empresas farmacéuticas, afectan a diversos aspectos, entre los cuales destacan:

- Mayor facilidad para reclutar a un grupo de voluntarios para poder realizar los ensayos necesarios antes de sacar al mercado nuevos medicamentos, lo que supone una aceleración del proceso.
- Los comités de ética, que desempeñan un papel muy importante en todo el proceso, se encuentran mucho más predispuestos a aceptar el proceso si en él se hallan involucradas tecnologías que potencien la privacidad.
- Una reducción importante de los problemas legales y posibles sanciones por incumplimiento de las normativas.
- La ventaja fundamental radica en que todo el proceso transcurre de una forma mucho más suave, lo que supone importantes recortes en los tiempos. Dadas las características de estos procesos, pequeñas reducciones de los tiempos suponen ahorros considerables de dinero. Por ejemplo, el retraso en una semana de una patente que tiene un valor de 5.000 millones de dólares estadounidenses (M$) viene a suponer un coste de 15 M€.
- Las mejoras en los desarrollos de medicamentos acaban teniendo un beneficio que repercute en toda la sociedad.
- Los voluntarios tienen garantizado su derecho a la intimidad en todo el proceso, a la vez que se benefician de los posibles usos que se puedan extraer de su información genética.

6.3 Aplicación de la identidad digital al ámbito de las aseguradoras de vehículos

En la actualidad, el modelo de facturación de muchos servicios se basa en patrones medios de consumo, en vez de en el consumo real llevado a cabo por cada usuario. Este modelo, que se utiliza principalmente por la imposibilidad de tener datos reales de cada uno de los usuarios, lleva implícito un mecanismo de compensación entre los usuarios. Así, los que utilizan dicho servicio de forma más intensiva son financiados en parte por aquellos que utilizan el servicio de forma menos intensiva.

El sector de los seguros de automóvil es un caso muy claro en el que se produce esta situación, ya que los criterios actuales que utilizan las aseguradoras para calcular la póliza que pagará el usuario

se basan en datos de carácter sociodemográfico del usuario y en las características del vehículo: edad y género del usuario, cilindrada y modelo del vehículo, tal y como se observa en la figura 44. Por tanto, la facturación final se basa en una serie de aspectos que poco tienen que ver con el riesgo real de cada una de las pólizas.

Figura 44. Variables utilizadas por las aseguradoras para el cálculo de la cuota del seguro del coche

Fuente: Elaboración propia.

Pay as you drive (PAYD) es un modelo de gestión de los seguros del automóvil que se basa precisamente en la idea de ajustar la cuota en función del uso, en este caso, de los kilómetros recorridos. Esto supone una ventaja tanto para la propia aseguradora, que así puede ofrecer ofertas más ajustadas y estar alerta de los usuarios que tienen mayor riesgo, como para los usuarios, que de este modo no tienen que pagar por los comportamientos arriesgados de otros conductores.

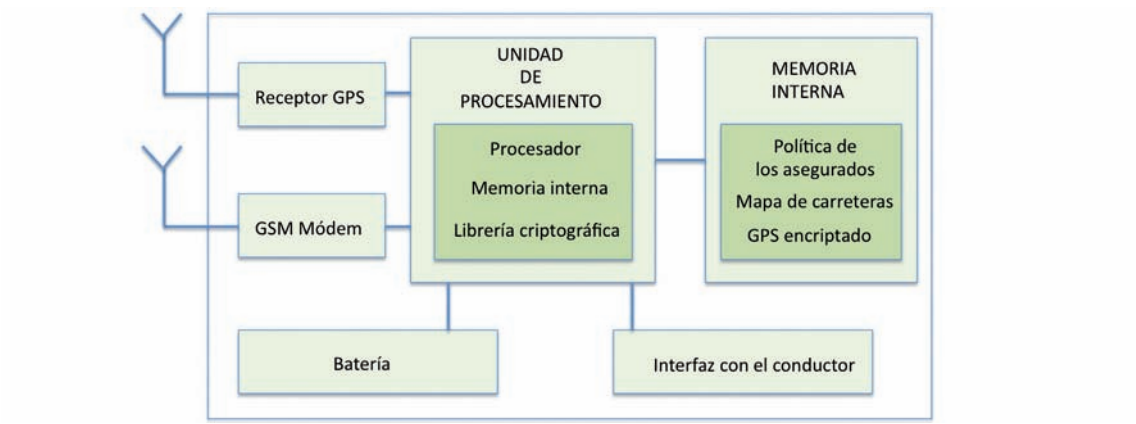
Hay que destacar que, en el caso concreto de PriPAYD, la recogida y gestión de los datos se puede realizar de varios modos:

- Los kilómetros pueden ser recogidos una vez al año en un lugar fijo (sin tener en cuenta la localización en la que se han realizado y manteniendo, por tanto, la privacidad). Además, otros sistemas basados en GPS comprueban que no se han superado los límites de velocidad en una carretera determinada, pero sin grabar la localización.
- Por otro lado, se puede llevar a cabo una recolección de los datos de localización mediante las lecturas en lugares colocados cerca de las carreteras, como por ejemplo en gasolineras. Esto permite una mayor riqueza de los datos, como pautas de comportamiento del usuario, tipo de viajes que realiza, tiempo de conducción sin parar, etc. Basándose en esa información, se pueden ofrecer descuentos a los conductores.
- También es posible recoger en tiempo real gran cantidad de datos, desde los de velocidad y posición, hasta otros datos útiles como la utilización del cinturón de seguridad, la ratio de aceleración, la observancia de las señales de tráfico, etc.

Esta categorización viene a demostrar que cuantos más datos se recopilan y más beneficio se puede obtener de ellos, mayores son los problemas de privacidad.

El caso de uso descrito, PriPAYD, elimina la necesidad de transferir datos sensibles personales con las aseguradoras. Para ello, traslada el almacenamiento y procesado de los datos desde un servidor externo al que podría acceder la compañía de seguros, hasta una caja negra situada dentro del propio coche (figura 45).

Figura 45. Caja negra de procesamiento de información para el cálculo de la póliza



Fuente: Balasch and Verbauwhede.

Con ello se quiere preservar la privacidad de manera que el coste de cada viaje sea calculado en tiempo real y agregado según se produce, y solamente estos datos de facturación sean los que se envíen al asegurador utilizando para ello tecnologías móviles. Los beneficios en el uso de este nuevo sistema, que incluye un alto nivel de privacidad en los datos referidos a la identidad del usuario que pueden ser más conflictivos, son bastante claros. En principio, tanto los usuarios como las empresas aseguradoras se beneficiarían de una mayor transparencia en los criterios de cálculo de las cuotas del seguro de los vehículos. Por otra parte, está demostrado que el uso de sistemas que penalizan el riesgo en el que incurren los conductores influye en los patrones de comportamiento de los usuarios, que suelen adoptar conductas menos arriesgadas con la consiguiente disminución de accidentes de tráfico y, por tanto, de víctimas. También los sistemas que penalizan el uso provocan una disminución en el empleo de los vehículos, lo que tiene efectos positivos en el medioambiente, además de reforzar el aspecto anterior (disminución del número de víctimas).

6.4 Aplicación de la identidad digital al ámbito de las empresas sanitarias

Durante los últimos años ha habido grandes inversiones en la actualización y modernización de los sistemas de información relacionados con la salud. La mayoría de los países de la UE han lanzado iniciativas que abarcan diversos ámbitos en este terreno, como la telemedicina, la conexión entre

centros de atención primaria y hospitales, o la digitalización del historial clínico. Todas estas iniciativas tienen una gran envergadura, tanto por la cantidad de usuarios, como por la complejidad y la variedad de la información que manejan, y por la gran cantidad de recursos que se requieren para su puesta en funcionamiento (figura 46).

Figura 46. Información digital en el ámbito sanitario

Fuente: Elaboración propia.

La gestión de la identidad de los pacientes, así como el respeto a las leyes de la privacidad, suponen un reto fundamental en el desarrollo de sistemas de información en el campo de la salud.

En la actualidad, hay compañías que están trabajando en el envío de información sanitaria de pacientes a registros nacionales de forma seudoanónima.

Un sistema como el propuesto aporta diversos beneficios a las empresas que lo utilizan. Por una parte, el inductor fundamental del uso de esta aplicación viene dado por la necesidad de cumplir con los estrictos requisitos que exige la administración en este campo. No obstante, son claros otros tipos de beneficios, como la reducción de costes y de la posibilidad de fugas de información con respecto a la utilización de métodos tradicionales, lo que supone también una disminución del número de demandas, procesos legales, etc.

Más adelante, estos métodos permitirán la interacción con terceras empresas manteniendo la privacidad. Este hecho podría facilitar mucho el proceso de acceder a servicios que necesiten información de carácter médico, como alergias, historial médico, y que pueden tener una influencia importante en la salud de los ciudadanos en situaciones determinadas como accidentes. Además, estos mecanismos pueden facilitar acciones positivas para el bien común de la sociedad sin desvelar la identidad de las personas estudiadas, como por ejemplo con fines de investigación y para luchar contra epidemias.

6.5 Aplicación de la identidad digital al ámbito de las empresas de información de riesgo crediticio

La gestión de la identidad digital es una actividad que cada vez adquiere más importancia y se espera que en el futuro tenga todavía una mayor relevancia dada la migración que se produce hacia la Red en una cantidad creciente de actividades personales.

Por ese motivo, no solo están naciendo un gran número de *start-ups* que tratan de posicionarse en este campo, sino que otras empresas con gran experiencia en el manejo de grandes volúmenes de datos de usuarios están explotando las posibilidades que ofrece la gestión de la identidad digital. Un ejemplo de esto es la empresa Experian, que lleva más de 30 años prestando servicios de información crediticia pero que ha ido adaptando su negocio según el desarrollo de Internet ampliando, por ejemplo, su oferta de servicios al área del marketing, desarrollando perfiles mediante información de usuarios de todo el mundo.

En el año 2011, Experian compró SafetyWeb, una empresa que permite a los padres controlar las actividades *online* de sus hijos. A su vez, un año antes SafetyWeb había ampliado su oferta de protección de la identidad digital para adultos con la adquisición de MyID, la cual se orienta a la creación de alertas en tiempo real tras la detección de fraude, robo de identidad o la exposición *online* no deseada de información personal, tal y como se muestra en la figura 47.

Figura 47. Funcionalidades de MyID

Fuente: Elaboración propia.

Experian, empresa ampliamente consolidada en la prestación de servicios crediticios, de toma de decisiones y de marketing, hace de esta manera una apuesta por la utilización de Internet para que los propios usuarios puedan controlar sus datos de forma interactiva. Con este fin, lanzaron el servicio CreditReport, que permite al usuario conocer la misma información que tienen los prestamistas a la hora de conceder un crédito, y también al servicio Protect MyID, que permite detectar el robo de identidades, así como la protección y la resolución del fraude. Este servicio incluye el escaneo de los números de cuenta, tanto de tarjetas de crédito como de débito, y la monitorización de los cambios de dirección.

Capítulo 7

Legalidad y privacidad

Desde que la información de clientes y usuarios se ha convertido en materia prima para las empresas, los riesgos para la intimidad que conlleva el tratamiento de sus datos van en aumento. La recogida y el tratamiento de la información personal de clientes o usuarios de los servicios web y de comercio electrónico, de los servicios en la nube (*cloud computing*) o en movilidad (*smartphone*), o de las cada vez más extendidas redes sociales, se está revelando como un aspecto especialmente sensible. A ello se une el carácter transnacional de Internet y la complejidad de aplicar normas homogéneas en todos los territorios, con tradiciones jurídicas y niveles de protección legales diferentes. Actualmente se están dando una serie de circunstancias (la regulación relacionada con la privacidad se torna más estricta, se publican noticias sobre abusos de empresas en este ámbito, la actividad del gobierno estadounidense en este sentido, así como la innovación tecnológica) que hacen que el usuario haya adquirido un mayor grado de conciencia sobre lo que es el mercado de datos masivos, y ello está creando a su vez un campo de cultivo para que las personas demanden servicios que ayuden a gestionar estos datos y que otorguen a su vez al consumidor un papel en este mercado.

Ya en la década de 1980, en un entorno muy diferente al actual, la Organización para la Cooperación y el Desarrollo Económico (OCDE) redactó ciertas directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales. En la actualidad, la discusión sobre la privacidad tiene que ver con la profunda transformación que está sucediendo, y precisamente este aspecto es especialmente vulnerable. Los principios de privacidad de la OCDE constituyen, hoy por hoy, a nivel internacional, un marco de privacidad comúnmente utilizado, lo que se refleja en las actuales leyes de privacidad y protección de datos o en los principales programas de prácticas y principios de privacidad adicionales. Estos principios son los siguientes:

- Principio de limitación en la recopilación: Establece que deberían existir límites en la recolección de datos personales, así como la obligatoriedad de obtener esta información de forma legal y justa, y bajo el conocimiento y consentimiento de la persona objeto de esta recopilación.
- Principio de calidad de los datos: Dispone que los datos personales deberán ser relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, exactos, completos y actuales.
- Principio de especificación del propósito: Declara que deberán especificarse los propósitos para los que se recogen los datos personales en el momento de su recolección y limita el posterior uso al cumplimiento de los fines declarados u otros compatibles con estos. También deberá notificarse cada vez que cambie la finalidad de la recolección de datos.
- Principio de limitación de uso: Los datos personales no deberán ser divulgados, puestos a disposición de terceros o utilizados con diferentes fines a los establecidos anteriormente, salvo ocasiones en las que el interesado dé su consentimiento y en las ocasiones en que lo exija la ley.
- Principio de medidas de seguridad: Los datos personales deberán estar protegidos por las correspondientes medidas de seguridad contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de estos.
- Principio de apertura: Deberá existir una política general de apertura sobre desarrollos, prácticas y políticas con respecto a los datos personales, así como los medios disponibles para comprobar la existencia y naturaleza de los datos personales, el uso de estos y la identidad y la residencia habitual del responsable del tratamiento.

- Principio de participación individual: La persona a la que hagan referencia los datos deberá tener el derecho a que se le confirme si el controlador de los datos tiene información que le concierne, y en caso de ser así, también tendrá derecho a que se lo comunique en un plazo y forma razonables, con un cargo, si lo hubiere, no excesivo, y de una manera inteligible. Además, tendrá derecho a que se le expliquen las razones por las que una petición suya, según los derechos anteriores, haya sido denegada, así como a poder cuestionar tal denegación. Por último, podrá expresar dudas sobre los datos relativos a su persona y, si su reclamación tiene éxito, conseguir que estos se eliminen, rectifiquen, completen o corrijan.
- Principio de responsabilidad: Determina que sobre todo controlador de datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios antes mencionados.

En líneas generales, estos principios establecen, por un lado, las condiciones de recogidas de datos justas, legales, con un límite y la necesidad de consentimiento por parte del titular de los datos personales, la persona de quien se recogen. A su vez, determinan la obligatoriedad por parte de los responsables del tratamiento de los datos a especificar el uso de estos en todo momento, prohibiendo un uso diferente al especificado y más concretamente, su divulgación. Además, la persona objeto de interés tendrá derecho a comprobar sus datos y la identidad del controlador, pudiendo en un momento dado pedir su eliminación o modificación.

Estos principios se recogieron en la 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. Desde entonces, la UE ha dictado varias normas al respecto, incluida la incorporación del derecho de protección de datos a la Carta de los Derechos Fundamentales de la Unión Europea (TÍTULO II – LIBERTADES – Artículo 8 – Protección de datos de carácter personal). Otras normas de interés son:

- 2001/497/CE: Decisión de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE.
- 2011/136/UE: Recomendación de la Comisión, de 1 de marzo de 2011, sobre directrices para la aplicación de las normas de protección de datos en el Sistema de Cooperación para la Protección del Consumidor (CPCS).
- Resolución del Consejo, de 18 de febrero de 2003, sobre un enfoque europeo orientado hacia una cultura de seguridad de las redes y de la información.
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).
- 2008/49/CE: Decisión de la Comisión, de 12 de diciembre de 2007, relativa a la protección de los datos personales en la explotación del Sistema de Información del Mercado Interior (IMI).
- Decisión n.º 1247/2002/CE del Parlamento Europeo, del Consejo y de la Comisión, de 1 de julio de 2002, relativa al estatuto y a las condiciones generales de ejercicio de las funciones de Supervisor Europeo de Protección de Datos.

- Acto del Consejo, de 28 de febrero de 2002, que modifica el Acto del Consejo de 12 de marzo de 1999 por el que se fijan las normas para la transmisión por Europol de datos personales a Estados y organismos terceros.
- Decisión 2009/917/JAI del Consejo, de 30 de noviembre de 2009, sobre la utilización de la tecnología de la información a efectos aduaneros.
- 2010/87/UE: Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo [notificada con el número C(2010) 593].
- Acto del Consejo, de 12 de marzo de 1999, por el que se fijan las normas para la transmisión por Europol de datos personales a Estados y organismos terceros.
- Decisión del Consejo de Administración de Europol, de 4 de junio de 2009, sobre las condiciones relativas al tratamiento de datos en virtud del artículo 10, apartado 4, de la Decisión Europol.
- 92/242/CEE: Decisión del Consejo, de 31 de marzo de 1992, relativa a la seguridad de los sistemas de información.
- Normas del Reglamento interno de Eurojust relativas al tratamiento y a la protección de datos personales (Texto adoptado por unanimidad por el Colegio de Eurojust en su reunión del 21 de octubre de 2004 y aprobado por el Consejo el 24 de febrero de 2005).
- Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS).
- Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.
- Recomendación de la Comisión, de 12 de mayo de 2009, sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia.
- Recomendación de la Comisión, de 26 de marzo de 2009, sobre directrices para la protección de datos en el Sistema de Información del Mercado Interior (IMI).
- Reglamento de Ejecución (UE) n.º 1179/2011 de la Comisión, de 17 de noviembre de 2011, por el que se establecen especificaciones técnicas para sistemas de recogida a través de páginas web, de conformidad con el Reglamento (UE) n.º 211/2011 del Parlamento Europeo y del Consejo sobre la iniciativa ciudadana.

La Directiva 95/46/CE se encuentra, en la actualidad, en proceso de revisión para incorporar, entre otras, las siguientes cuestiones:

- Su aplicabilidad directa tomando la forma de Reglamento, para evitar aplicaciones diferentes por parte de los Estados miembros como ha ocurrido con la vigente Directiva.

- Ampliación del alcance jurisdiccional: El nuevo Reglamento no solo se aplicaría a las empresas establecidas dentro de la UE, sino también a cualquier empresa con sede fuera de la UE que ofreciese bienes y servicios a los residentes de la UE y, por lo tanto, procese los datos personales de estos. Cualquier empresa de este tipo tendría que nombrar a un representante en la UE, a menos que el número de sus empleados sea inferior a 250.
- Notificación de vulneración de datos en menos de 24 horas: El Reglamento obligaría a las empresas a notificar a la autoridad nacional de protección de datos las pérdidas de datos «sin dilaciones indebidas y, cuando sea posible, a más tardar en las 24 horas después de haber tenido conocimiento de ello». Por otra parte, si la notificación no se realiza dentro de las 24 horas, la notificación tiene que ir acompañada de «una justificación razonada».
- Consentimiento explícito: El Reglamento obligaría a las empresas a obtener un consentimiento «específico, informado y expreso» de los individuos antes de recoger o utilizar sus datos personales.
- Aumento de las multas: Con arreglo al Reglamento, las autoridades nacionales de protección de datos tendrían la autoridad para multar a los infractores con hasta 1 millón de euros, o para el caso de las empresas, con el 2 % del volumen de negocios anual a nivel mundial.
- Derecho al olvido: El Reglamento exigiría que las empresas, en la mayoría de los casos, borraran los datos personales de los individuos cuando así lo soliciten. Las empresas tendrían que eliminar esos datos personales que se publican en Internet e «informar a terceras partes que estén procesando esos datos» con el fin de que procedan, también, a su eliminación.

En el caso español, la Constitución de 1978 incluyó, en el artículo 18 dedicado al derecho a la intimidad, honor y propia imagen, un segundo párrafo que eleva a rango de derecho fundamental el *habeas data* o el derecho de los ciudadanos de control y persecución de sus datos personales allí donde se encuentren. Este derecho se vio inicialmente desarrollado por la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) que fue sustituida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y desarrollada por Real Decreto 1720/2007, de 21 de diciembre, que establece su Reglamento. Mediante la adopción de la LOPD, se ajustaba el derecho de protección de datos en España a lo preceptuado en la Directiva 95/46/CE. El derecho a la protección de datos personales incluye, en la actualidad, no solo la exigencia de que la recogida de los datos haya de hacerse mediando un consentimiento informado del afectado (titular de los datos), sino que se fundamenta en el control que sobre estos tiene durante el ciclo de vida de los datos, mediante el ejercicio de los derechos ARCO, esto es, de acceso, rectificación, cancelación y oposición al tratamiento (por ejemplo, a las finalidades de marketing).

En el marco de las comunicaciones electrónicas se han desarrollado recientemente nuevas reglas que debían haberse adaptado al derecho interno de los Estados miembros el pasado mes de mayo de 2011. Dichas reglas se concretan en las siguientes:

- Notificación de *data breach* o de pérdidas de datos personales: Esta norma obliga tanto a las operadoras de telecomunicación como a los proveedores de servicios en Internet, a tomar fuertes medidas de seguridad para proteger los nombres, direcciones de correo e información

bancaria de sus clientes, así como toda llamada telefónica y sesión *online* en la que tomen parte. A su vez, con el fin de incentivar a los proveedores de redes y servicios de comunicaciones a la mejor protección de los datos personales, estas reglas obligan a notificar sin demoras indebidas la pérdida o robo de la información personal, tanto a las autoridades de protección de datos como a los clientes.

- La *cookie law*, o las reglas europeas orientadas al cumplimiento del principio *do not track*: El operador, tanto de los servicios web como de las plataformas de publicidad, ha de obtener el consentimiento de los usuarios para servirle las *cookies* y ha de informar del uso que de ellas se va a realizar. En concreto, en el caso de datos no relacionados con el servicio al que accede el usuario, las nuevas normas obligan a los Estados miembros a garantizar que los usuarios den su consentimiento informado sobre la finalidad de la recogida antes de que se acceda a estos datos o sean almacenados.
- *Spam*: Las reglas relacionadas con el *spam* (los *e-mails* comerciales no solicitados) refuerzan y aclaran los requisitos legales para luchar contra este. Más concretamente, de ahora en adelante todos los *e-mails* comerciales que no contengan información completa acerca de la compañía remitente son considerados ilegales. En este sentido, ya que muchos *spammers* operan entre fronteras, la cooperación entre autoridades es muy importante. Es más, las nuevas normas dan a los proveedores de servicios de Internet el derecho a proteger sus negocios y a sus clientes tomando acciones legales contra los generadores de *spam*[38].

38. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/320&format=HTML&aged=0&language=EN&guiLanguage=en

Capítulo 8

Encuentro con expertos

La realización de este informe ha contado con la colaboración de un grupo de expertos en diferentes ámbitos, quienes han aportado una visión complementaria al análisis de la identidad digital. Este apartado recoge la transcripción literal de la reunión que tuvo lugar el día 10 de febrero de 2012 en la sede de Fundación Telefónica en Madrid.

El análisis de una versión inicial del documento y el planteamiento de una serie de preguntas a los profesionales convocados fueron el punto de partida de dicha reunión, en la que, además de las respuestas a estas, también tuvo cabida una exposición individual de cada uno de los expertos y un debate conjunto.

Ilustración 1. Encuentro de expertos sobre identidad digital.

8.1 Punto de vista sociológico-psicológico

Dolors Reig
Consultora y profesora de psicología social

Preguntas de las que partió su intervención:

- La creciente actividad de las personas en la Red está contribuyendo a la creación de un rastro digital cada vez mayor. ¿Hasta qué punto influye todo ello en la propia configuración de la identidad y en el comportamiento humano? ¿Y cómo afecta esto a la sociedad?

Cada vez más, vamos evolucionando conforme la tecnología evoluciona y ello nos hace, en cierto sentido, más grandes.

Voy a comenzar mostrando una presentación porque estamos en la edad de la imagen y hay cosas que se expresan mejor con imágenes que con palabras. De hecho, lo que estoy haciendo es apoyarme en una parte de mí que de momento no puedo proyectar de otro modo que no sea este. Yo creo que esto es una parte importante de esa identidad digital, ya que cada día más somos «nosotros y nuestras tecnologías». Siempre hemos sido nosotros y nuestras tecnologías: aquellos que utilizan gafas son «ellos y sus tecnologías» desde hace ya tiempo. Sin embargo, cada vez más, vamos evolucionando conforme la tecnología evoluciona y ello nos hace, en cierto sentido, más grandes.

Respecto al tema de si Internet nos hace más listos o más tontos, lo último que he leído planteaba un escenario casi de ciencia ficción, donde podrían conectarse electrodos de baterías ya pre-

paradas directamente al cerebro, lo que haría más inteligentes a los jóvenes. Esta hipótesis viene refrendada por algunos estudios que demuestran que, en efecto, estas baterías ayudan al proceso de aprendizaje. O sea el nivel de *cyborgs* que somos va ampliándose más. Para mí, este, repito, un escenario de casi ciencia ficción y lo de las baterías me parece incluso peligroso, pero realmente dicen que sí y que de momento, además, no hay riesgo de que estemos quemando las neuronas, sino que los electrodos lo que hacen es reforzar las sinapsis cerebrales. Cuando uno el concepto de *cyborgs* y el ordenador podemos ir mucho más allá de esto y, de hecho, ya estamos yendo mucho más allá.

Ilustración 2. Dolors Reig.

Quería sugerir una frase que se aplica muy bien al contexto actual. Es de Zygmunt Bauman, autor que me gusta mucho, dice así: «La construcción de identidad implica el triple desafío (y riesgo) de confiar en uno mismo, en otros y también en la sociedad».

Evidentemente, no habla de la identidad digital, ya que se trataba de otra época, pero puede aplicarse a la actualidad. En mi opinión, este último punto, que quizá ya se cumplía en el pasado, se hace aún más importante con las nuevas redes sociales dada la necesidad de confiar en otros y en la sociedad. En determinados momentos de la historia uno dependía en mayor grado de sí mismo.

El éxito de la web social está garantizado porque somos sociables por naturaleza.

En primer lugar, cuando estamos hablando de redes sociales y de cómo nos cambian hay que destacar un aspecto esencial. El otro día alguien me preguntaba: «¿Cuándo va a bajar esto de la Web 2.0?». La respuesta es: cuando dejemos de alimentarnos, es decir, la sociabilidad es una necesidad básica del ser humano. El éxito de la web social está garantizado porque somos sociables por naturaleza. Después de las necesidades de comer, de seguridad, de tener un lugar donde vivir..., lo siguiente que nos motiva a los seres humanos, mostrado en la pirámide de motivación de Maslow (Ilustración 3), son aspectos más sociales, como el amor, la autoestima, la autorrealización personal que se produce cuando el grupo te reconoce, te reafirma... Creo que este es un elemento impor-

tante, sí, somos sociables por naturaleza, y el contexto actual y las tecnologías están ampliando las posibilidades y su alcance a un nivel que todos conocéis.

Ilustración 3. Pirámide de motivación (Maslow).

También me preguntan muchas veces: «¿Hay lugar para otra red social?». Yo creo que hay lugar para infinitas redes sociales más porque nuestra sociabilidad es muy potente. Clay Shirky habla de excedente cognitivo. Pienso que también hay excedente social, también teníamos muchísimas ganas de volver a compartir cosas, de recuperar esa sociabilidad en algunos momentos perdida.

En la Ilustración 4 podemos ver una comparación de mi yo real y mi yo digital. Es un gráfico antiguo, en mi opinión, deberían ir vestidos igual, ya que una de las claves de la evolución de la identidad digital es que somos cada vez más auténticos en redes sociales.

Una de las claves de la evolución de la identidad digital es que somos cada vez más auténticos en redes sociales.

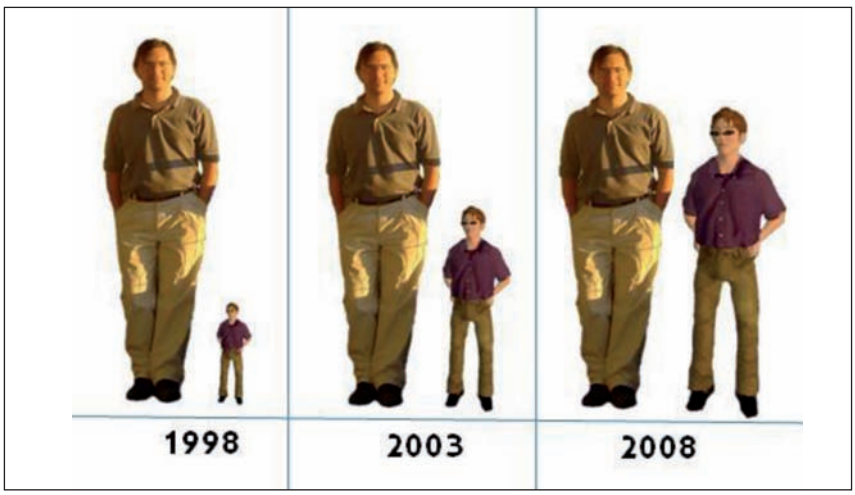


Ilustración 4. Yo real frente a yo digital.

Podemos ver la evolución de las identidades digital y real, cómo va aumentando, hasta el punto de que hoy en día, en mi caso, por ejemplo, mi yo digital es inmensamente más grande que mi yo real.

Al final, «identidad» y «social» creo que están absolutamente unidas, lo que constituye la base de mi argumento. Internet nos está ampliando no solo tecnológicamente, en el sentido de *cyborg*, sino también en sentido de ser social. Si yo soy mi grupo social, en la actualidad soy mucho más grande que en el año 1998 y cada vez voy a ser más grande, gracias a esa interacción social que cada vez va a ser más grande en calidad y en cantidad.

Las redes sociales nos cambian, cambian nuestra identidad, la amplían.

La experiencia en Internet se vive como real y nos cambia. Como dijo Manuel Castells: «No somos los mismos desde que estamos en redes sociales». Esta frase la formuló cuando tuvieron lugar las revoluciones en los países árabes. Creo que es muy acertada: no somos los mismos desde que estamos en redes sociales, las redes sociales nos cambian, cambian nuestra identidad, la amplían. Como comentaba anteriormente, dejan que potenciemos toda esa sociabilidad y añadiría que ello no es algo nuevo, sino que volvemos a ser lo que un día fuimos, volvemos a las ágoras públicas, de las que, en cierta manera, la televisión y otros medios de comunicación nos habían apartado.

La información vuelve a ser muy social y soy de la opinión de que no somos los mismos, pero no somos tan nuevos. Mi abuela lo hubiera entendido muy bien y mi madre no lo entiende muy bien. Y es que mi madre se cree lo que dicen en la televisión mientras que mi abuela se creía lo que decían en el pueblo. Hemos recuperado de alguna forma ese carácter de información en lo social.

¿Cómo de distintos somos en lo social?, ¿cómo nos cambia?, ¿en qué punto somos diferentes?

Nos acostumbramos a compartir más, yo creo que es indudable. En la formación que imparto a la gente más mayor que no conoce todo esto, les sorprende muchísimo el hecho de compartir, compartir fotos, compartir entradas de post... Los descoloca y les encanta, y ven posibilidades. Si empezamos a compartir de este modo el mundo va a cambiar.

Nos hacemos más participativos y empoderados. Se habla de tecnologías de la participación como las TIC (tecnologías de la información y la comunicación), las TAC (tecnologías del aprendizaje y del conocimiento) –este último es un término inventado por la Generalitat de Cataluña y a mí me parece adecuado–... Yo siempre digo que hay que reivindicar las TEC (tecnologías del empoderamiento y de la capacitación).

Relacionado con la eCiudadanía, ¿para qué la identidad?, ¿solo desde el punto de vista de la seguridad de la privacidad, solo para proteger aspectos, derechos básicos o también para ampliarlos? ¿Cómo sería el caso de la eCiudadanía?

Creo que, al final, en las redes sociales acabamos siendo más responsables, aunque esto es algo que queda por demostrar. Los psicólogos siempre decimos que cuanto más control tienes de fuera, menos control tienes de dentro. Los educadores, sobre todo, lo recalcamos mucho en relación con la educación de los hijos. En el fondo, el hecho de estar solos, de interactuar de esta forma, teniendo el círculo social al otro lado de una pantalla, en el fondo y contra todo pronóstico puede llegar a hacernos más responsables y no menos, aunque también, en determinados momentos, puede llegar a hacernos menos responsables.

En la Ilustración 5 se muestran los principios de Internet.

Ilustración 5. Evolución de la transparencia en Internet.

La primera imagen corresponde a los primeros chats. En la actualidad, se tiende a ser más transparente, como pone de manifiesto la segunda imagen.

Me viene a la memoria una charla con un grupo de chicos en la que hablábamos de jóvenes y tecnologías. Una persona del público les preguntó si alguno se había hecho pasar por otra persona en Internet y recuerdo la cara de uno de ellos. Todos se pusieron muy nerviosos, pero uno de ellos en concreto se puso rojo como si alguien le hubiera preguntado en su lugar «¿Le has pegado alguna vez a alguien?», «¿Has matado alguna vez a alguien?». Es decir, realmente, es algo grave, feísimo, en su propia etiqueta, en su propia forma de andar por la Red, lo de hacerse pasar por otro.

Por ello creo que todo el tema de criptografía de seguridad es muy importante hoy en día: hay generaciones que se han socializado con una idea de la privacidad mucho más cerrada, pero esto va a ser cada vez menos importante. Evidentemente, considerando a un ser humano cada vez más responsable –y ahí volvemos a lo mismo– puede que sea una utopía.

En las redes sociales mostramos nuestro verdadero yo.

Estoy convencida de que en la evolución de la identidad digital, desde el principio, ha habido una tendencia a mayor transparencia. De hecho, los estudios parecen decir que, en efecto, en las redes sociales mostramos nuestro verdadero yo, salvo excepciones de patologías, de neurosis... Pero en general, los chavales se amplían y no fingen ser alguien distinto. Si hablamos de ámbitos profesionales todavía más: cuanto más te presentes como tu verdadero yo, más posibilidades habrá de que todo vaya bien.

Creo que eso es lo que somos hoy en Internet: soy lo que comparto, lo que produzco, las instituciones con las que trabajo y, sobre todo, soy con quien me relaciono. Por eso soy cada día más grande.

8.2 Punto de vista de desarrollo de negocio

José Antonio Gallego
Asesor de Procesos en Visa Europa

Preguntas de las que partió su intervención:

- Para cualquier empresa, la correcta gestión de la relación con el cliente así como su profundo conocimiento se revelan como actividades básicas para el desarrollo del negocio. ¿Hasta qué punto no incorporar este análisis de una manera sistemática, haciendo uso de esta identidad digital, puede afectar a la propia evolución de las empresas y organizaciones? ¿Qué potencial de desarrollo económico tiene esta tendencia y qué beneficios puede aportar al usuario?

El pago de bienes y servicios es una necesidad primaria de la persona. Si nos remontamos a la década de 1950, cuando se inventaron las tarjetas, vemos que nacieron con objeto de dar prestigio a quien las portaba. La tarjeta significaba que aquel individuo pertenecía a un determinado club selecto y, por lo tanto, había sido considerado solvente por una serie de empresas y personas.

La tarjeta da una garantía al comercio que permite realizar una actividad de otra manera inviable.

Las tarjetas fueron evolucionando hasta convertirse en una muestra de la identidad de la persona. Por ejemplo, una persona de un pueblecito puede ir a Nueva York y pagar sin ningún problema con su tarjeta porque realmente es como si la conocieran gracias a ella. Hoy en día la tarjeta da una garantía al comercio que permite realizar una actividad de otra manera inviable. Esta funcionalidad, además, fue asociándose a la garantía de pago. Al comercio realmente no le importa quién seas, lo que quiere es venderte y para hacerlo lo que necesita es una garantía. Por esta razón empezaron a desarrollarse reglas que en la actualidad siguen vigentes y que van cambiando a la par de la evolución de las tecnologías.

Una vez llegados a este punto, el comercio se sentía seguro, ya que la tarjeta presentaba una garantía de que iba a cobrar. Sin embargo, unido a la evolución de las tecnologías, empezó a surgir el fraude, es decir, alguien lograba reproducir tu tarjeta, suplantaba tu identidad y pagaba con tu dinero. A pesar de la existencia de seguros, esto suponía un problema y, por ello, la tecnología se puso al servicio de combatir el fraude.

Fue entonces cuando surgieron las tarjetas de banda magnética, que estuvieron funcionando durante muchos años, de hecho todavía las llevamos en la cartera. La banda magnética evitaba el fraude masivo o el fraude fácil, ya que requería disponer de un lector, estar conectado a un sistema más o menos seguro... No obstante, a lo largo del tiempo aquellos que se dedican al fraude también hicieron uso de la tecnología y aprendieron a cómo seguir haciéndolo a pesar de la banda.

Ello condujo a la implementación de un chip en las tarjetas, cuya criptografía asimétrica hace muy difícil que nadie pueda usarla de forma fraudulenta, aspecto importantísimo para el mundo presencial. Sin embargo, aparece Internet y empieza a crecer toda la actividad en este entorno –la necesidad de pagar es mayor o incluso mayor que la que se experimenta en el mundo físico–, pero con el inconveniente de que de nada sirve tener tarjetas con banda o tarjetas con chip ya que, de momento, la forma de introducir los datos consiste en teclear un número a mano. Ello no impide que se cometa fraude y, en consecuencia, tanto la gente como los comercios fueron muy reacios a utilizar Internet en sus compras y ventas al principio. De hecho, en los inicios de Internet, muy pocos comercios entran *motu proprio* y solo aquellos que se ven forzados lo hacen. Actualmente esta tendencia está cambiando.

De nada sirve tener tarjetas con banda o tarjetas con chip ya que, de momento, la forma de introducir los datos consiste en teclear un número a mano.

Por otro lado, salen a la luz fraudes millonarios que provocan que las entidades financieras no apuesten por este negocio y pongan muchas trabas a la apertura de comercios en la red de forma segura, entendiendo por forma segura que el comercio está protegido: es la entidad emisora la que asume el riesgo, pues está garantizando la identidad de ese cliente.

Ilustración 6. José Antonio Gallego.

El DNI-e se trata probablemente de una de las mejores herramientas que tenemos hoy en día como prueba de identidad y seguridad.

Todo ello supone un cambio importantísimo y la necesidad de desarrollar tecnologías que hagan seguro el comercio en la Red. Así, en los últimos años se ha desarrollado una serie de tecnologías que permiten el comercio con cierta seguridad, de hecho, aunque el fraude existe, está controlado y supone alrededor del 0,02 % del comercio electrónico, que es algo que puede asumirse. Para mejorar aún más la seguridad, Visa va a sacar un nuevo producto que eliminará la necesidad de que el número de la tarjeta viaje por la Red gracias a la creación de un repositorio securizado.

Lo más importante en este sentido es la comodidad y que el cliente perciba seguridad; este segundo ingrediente es vital. Una demostración de ello es el DNI-e, que se trata probablemente de una de las mejores herramientas que tenemos hoy en día como prueba de identidad y seguridad, pero lamentablemente todavía no se ha extendido su uso porque la gente no ha entendido plenamente para qué sirve y las empresas privadas tampoco han fomentado mucho su utilización. Por consiguiente, creo que va a haber un cambio radical. En el caso del comercio electrónico las ventas se están disparando, aunque todavía pueden crecer más. España es un país muy maduro en cuanto a medios de pago, aunque el comercio electrónico no supone más que el 4 % de las ventas totales con tarjeta, mientras que en el Reino Unido, por ejemplo, está en el 28 %. El motivo de este dato es que en España no hay oferta. Ahora mismo la Comunidad de Madrid está intentando incentivar al pequeño y mediano comercio para que se animen a entrar en Internet, puesto que se trata de una forma de comercio relativamente barata en la que no se necesitan grandes inversiones en locales.

España es un país muy maduro en cuanto a medios de pago, aunque el comercio electrónico no supone más que el 4 % de las ventas totales con tarjeta.

Para terminar, me gustaría comentar que lógicamente Visa está muy interesada en apoyar cualquier iniciativa que permita que la identidad del cliente no se pueda suplantar. Consideramos este un punto fundamental, por lo que trabajaremos e invertiremos lo que sea necesario para permitir que la sociedad pueda disfrutar de un bien necesario de una forma totalmente segura.

8.3 Punto de vista de las Fuerzas y Cuerpos de Seguridad del Estado

Juan Crespo
Director general de la Policía

Guillermo Reyes
Comandante de la Guardia Civil

Preguntas de las que partieron sus intervenciones:

- El ejercicio de los derechos fundamentales, su preservación y protección se enfrenta a una serie de conflictos, entre ellos el clásico dilema entre seguridad y libertad. En el marco de la actividad en Internet este tipo de conflictos se pone si cabe aún más de manifiesto. ¿Cómo actúan las Fuerzas y Cuerpos de Seguridad del Estado para proteger la seguridad de las personas en la Red? ¿Qué recomendaciones deberíamos seguir para gestionar adecuadamente nuestra identidad en la Red? ¿Es suficiente la normativa actual para perseguir el ciberfraude y el cibercrimen?

Juan Crespo:

La identidad es una de las primeras preocupaciones del ser humano como individuo, lo primero es la conservación de sí mismo y después la de la especie. Pero una vez que ya tiene solucionada su propia conservación empieza a identificarse o a distinguirse del resto del grupo. Lo hace a través de características que le permiten distinguirse, al principio, las físicas.

La policía comienza a realizar los padrones de domicilio a inicios del siglo XIX. Una de sus funciones era la de entregar un salvoconducto al ciudadano para que cuando viajara supieran quién era. En un principio, el individuo solo se relacionó con su entorno, por lo tanto, no era necesaria la existencia de un agente de la confianza de todos que garantizara su identidad. Poco a poco esos documentos de identidad, inicialmente simples folios, fueron evolucionando e incorporaron las medidas de seguridad necesarias para evitar suplantaciones de identidad.

Nuestra identidad puede estar en cualquier sitio y no es una identidad física, sino una identidad basada en una serie de perfiles o de comportamientos en Internet. Esta expansión de la identidad implica que sea mucho más difícil el proceso de autenticación.

Hoy en día nos encontramos en la sociedad de la información, donde el ámbito de aplicación de la identidad de una persona se ha vuelto a ampliar y ya no tiene límites. Nuestra identidad puede estar en cualquier sitio y no es una identidad física, sino una identidad basada en una serie de perfiles o de comportamientos en Internet. Esta expansión de la identidad implica que sea mucho más difícil el proceso de autenticación. El documento de identidad electrónico contribuye a solucionar estas dificultades: nos brinda la posibilidad de dar una orden de pago a un comercio para que la envíe a la entidad de pago sin necesidad de introducir los datos de la tarjeta.

Lo que hizo la Policía Nacional para poder fomentar el desarrollo de la sociedad de la información fue comprobar qué tecnologías existían en ese momento que reunieran los requisitos de seguridad necesarios y permitieran al ciudadano estar en posesión de los elementos requeridos para realizar una firma con un bolígrafo y que nadie fuera capaz de quitarle ese bolígrafo y hacer una firma exactamente igual. Acudimos a la Fábrica Nacional de Moneda y Timbre, que contaba con personal experto en tarjetas, y al Centro Criptológico Nacional, donde están algunos de los mejores expertos del país en criptografía, y pedimos que evaluaran la seguridad del desarrollo, que hacía lo que tenía que hacer y no nada más, de tal manera que no existiera ninguna vulnerabilidad. Seleccionamos las mayores longitudes de claves públicas que se podían elegir entonces –el DNI utiliza claves de 2.048 bits mientras que la tarjeta con una fortaleza mayor utiliza 1.024 bits–, e implementamos los algoritmos de firma más fuertes que había y que soportaran al resto de los interlocutores. Además, la Policía Nacional se mantiene en constante evolución y estudia las nuevas tecnologías; de hecho, ya se ha pedido a la Fábrica de Moneda y Timbre que prepare el sustituto al chip actual, de modo que esté preparado antes de que la tecnología actual sea vulnerable. De esta forma nuestros ciudadanos dispondrán de las herramientas más seguras en cada momento.

El DNI utiliza claves de 2.048 bits mientras que la tarjeta con una fortaleza mayor utiliza 1.024 bits.

Ilustración 7. Juan Crespo.

Actualmente España tiene más tarjetas de identidad electrónica que el resto de los países que conforman la Unión Europea.

El despliegue del documento de identidad electrónico comenzó en el año 2006, cuando había tres países más que iniciaban este tipo de proyecto y actualmente España tiene más tarjetas de identidad electrónica que el resto de los países que conforman la Unión Europea. Alemania comenzó el año pasado, en noviembre de 2011, a emitir su tarjeta de identidad electrónica, pero no es una emisión global ni incluye el documento electrónico si no se solicita expresamente. Sin embargo, en el caso español en un solo acto se adquiere el documento físico y el electrónico.

Por otro lado, respecto al problema que se ha comentado acerca de su uso y que se plantea siempre que se habla del DNI electrónico, podemos decir que la Administración ha hecho un gran esfuerzo por poner en la red todos los servicios que eran presenciales, de forma que para los administrados no haya ni tiempo ni lugar para ejercitar esos derechos, y puedan así reclamar el ejercicio de los mismos cualquier día del año a cualquier hora. El problema es que, a pesar de que existe una ley de medidas de impulso para las tecnologías de la información que obliga a las grandes empresas a desarrollar los accesos con el DNI electrónico, esta es una norma que obliga pero no castiga, por lo que muchos no han implementado los servicios y los pocos que lo han hecho ha sido para poder «cubrir el expediente».

La tecnología existe, es factible, pero es necesario hacer un esfuerzo, ya que permitiría a los comercios evitar el repudio de algunas de sus operaciones y, además, evitaría ese 0,02 % de fraude.

Así, a veces hay quejas sobre que el lector es caro o que no se encuentra fácilmente: en efecto, 10 euros puede ser dinero pero si se va a comprar por Internet no es mucho, sobre todo si tienes un ordenador que te ha costado 500 euros; además, en la actualidad sí se encuentra fácilmente en el mercado. El problema es que no hay servicios, sobre todo servicios que se hacen diariamente como la compra de un billete de avión, mientras que otros, como la solicitud de una beca, el empadronamiento..., que una persona realiza con poca frecuencia, sí lo están. Yo he visto en estos últimos días dos aplicaciones para utilizar el DNI electrónico en dispositivos móviles, basadas en la utilización de tecnologías de radiofrecuencia o *bluetooth* para traspasar al lector la orden de firma del documento que hay que firmar. La tecnología existe, es factible, pero es necesario hacer un esfuerzo, ya que permitiría a los comercios evitar el repudio de algunas de sus operaciones y, además, evitaría ese 0,02 % de fraude.

José Antonio Gallego: La gran ventaja del uso del DNI electrónico se encuentra en la autentificación de la identidad, ya que hasta ahora esta actividad es realizada por los dependientes de los comercios, quienes no son especialistas en verificar identidades. Si, por el contrario, yo me identifico con mi DNI electrónico, quien realmente me está identificando es el Gobierno de España.

Si yo me identifico con mi DNI electrónico, quien realmente me está identificando es el Gobierno de España.

Juan Crespo: La Administración no solo participa en la emisión del documento de identidad, sino también en la validación de la identidad electrónica. En el momento que tú realizas una transacción, para que esta sea válida hay que hacer tres cosas:

1.- Ver que los certificados están vigentes.

2.- Ver que no están revocados, para lo cual hay que consultar a la autoridad de validación que esos certificados no están en una «lista negra».

3.- Ver que el documento que se ha firmado no ha sido manipulado ni modificado.

Con eso, toda transacción goza de todas las garantías legales iguales a la firma manuscrita.

Antonio Castillo: A mí hay un tema que me llama la atención. Por una parte se promueve el uso del DNI electrónico, sin embargo, la propia Administración tiene una serie de reglas y sigue pidiendo otro tipo de identificaciones. Por ejemplo, cuando alguien va a abrir una cuenta bancaria, lo primero que le hacen es fotocopiar el DNI. Fotocopiar un DNI digital no tiene mucho sentido, incluso en el chip de los DNI se puede almacenar mucha información, lo que permitiría que el ciudadano no tuviera que recurrir a distintos certificados emitidos por diferentes organismos con sus tasas correspondientes.

Juan Crespo: La ley 11 de 2007 de acceso de los ciudadanos a los servicios públicos que mencionaba anteriormente establecía que los servicios no solamente tenían que prestarse sino rediseñarse. Había que estudiar uno a uno cada uno de los servicios y ver cómo se podían transponer, ya que para muchos servicios en papel, su adaptación al mundo electrónico supone un rediseño. Hay cosas que estamos haciendo en este sentido, por ejemplo cuando tú vas a solicitar un DNI por primera vez se pide una partida de nacimiento, un certificado de empadronamiento, además de la presencia de los padres. Desde el año 2007 el certificado de empadronamiento no es necesario, puesto que estamos conectados con el INE; el certificado de nacimiento lo seguimos pidiendo aunque estamos a punto de conectarnos con el Ministerio de Justicia para que ese documento no sea necesario. Hay que tener en cuenta que la ley de administración electrónica tenía un apartado donde decía «sin incremento del gasto». Realmente no es así, informatizar un sistema sin incrementar el gasto es imposible, por eso la Administración está realizando importantes esfuerzos para lograr esta informatización en una época en la que la reducción del gasto ha sido cada vez mayor, mientras las exigencias de prestación de servicios por parte de la Administración y por parte de los políticos son cada vez mayores. Poco a poco vamos dando pasos para suprimir esos documentos que pide la Administración y que puede conseguir por sus medios. El ejemplo del Banco de España es otra entidad más que poco a poco tendrá que ir modificando los procedimientos.

Para muchos servicios en papel, su adaptación al mundo electrónico supone un rediseño.

La Administración está realizando importantes esfuerzos para lograr esta informatización en una época en la que la reducción del gasto ha sido cada vez mayor.

Guillermo Reyes

El delito se ha transformado, ha evolucionado y se ha adaptado a las nuevas tecnologías, como pasa prácticamente con todo delito.

Cuando se hace uso de las buenas prácticas no se suele tener problemas en la sociedad; el problema surge, en concreto, en el área de la identidad digital, cuando se hace un uso indebido de la misma. Al hilo del tema de la usurpación o suplantación de la identidad que se ha comentado anteriormente, el delito se ha transformado, ha evolucionado y se ha adaptado a las nuevas tecnologías, como pasa prácticamente con todo delito.

Me gustaría hacer una aclaración en cuanto a lo que supone la suplantación de la identidad. Esta supone el tráfico y el uso de una identidad que no corresponde; en cambio, el fraude de identidad supone el uso de una serie de datos personales para cubrir actividades delictivas.

En este sentido –y adentrándome en el mundo de las redes sociales, en el que este aspecto no está claro para los usuarios–, antes de hacer uso del servicio, las redes sociales lanzan preguntas del tipo «¿Este es su perfil y accede a él?», «¿No es su perfil y alguien se está haciendo pasar por usted?» y, por lo tanto, ese perfil es falso. Esto nos da una idea de lo que entendemos por robo de identidad: nos estamos haciendo pasar por alguien que realmente no existe o probablemente existe y lo utilizamos para cometer un acto delictivo. Entonces, ¿qué es la suplantación de la identidad? Hacerse pasar por otra persona, sea esta real o ficticia. El gesto puede ser reprochable en determinados ámbitos pero en el delictivo es decisivo que se utilice como medio para realizar algún tipo de delito.

Durante el año 2011 tenemos constancia de 239 hechos con tipología «usurpación de la identidad» donde el medio utilizado ha sido Internet.

Realmente, cuando hablamos de suplantación de identidad hacemos referencia a una serie de actividades que en sí mismas pueden suponer un acto delictivo, como por ejemplo la adquisición no autorizada de bases de datos personales, su transferencia, manipulación o alteración, o su uso mediante la falsificación de la identidad para evitar dar la identidad real de un delincuente. Estadísticamente, en el ámbito de la Guardia Civil durante el año 2011 tenemos constancia de 239 hechos con tipología «usurpación de la identidad» donde el medio utilizado ha sido Internet. Hasta ahora hemos hablado de los que son delitos porque no todos se consideran delitos, sino que pueden considerarse como falta.

¿En qué consisten los hechos delictivos? La mayor parte de ellos tienen lugar en las redes sociales y consisten en hacerse pasar por otra persona y crear una cuenta con su nombre con el objetivo de desacreditarla a ella o a una persona de su entorno. Los motivos suelen ser diversos, entre ellos la venganza. También consisten en actividades económicas como pudiera ser la venta de vehículos, en un número que llama la atención, o la contratación de servicios de telefonía. Otro tipo de delitos son el robo de tarjetas para realizar compras por Internet, un delito que suele cometerlo gente de confianza dentro de la casa. En líneas generales, estos son los delitos que tenemos en la base de datos de la Guardia Civil.

Esto nos lleva a preguntarnos: ¿quién puede ser objeto de una suplantación de identidad? La respuesta es: cualquiera, no es necesario ser famoso ni salir en la televisión.

Ilustración 8. Guillermo Reyes.

Algunas de las formas en que se obtienen estos datos, al margen del robo de tarjetas o identificación, son el *phishing* y el *spoofing*. El *phishing* se basa en obtener información confidencial de las víctimas por distintos medios, ya sea con mensajes fraudulentos o mensajería instantánea o con falsificación de sitios web. Cada vez tenemos más conciencia de las medidas de seguridad que debemos seguir por Internet para valorar si una página es falsa.

Dentro del *phishing* aparecen cuatro modalidades. Se utiliza el *phishing* para la creación de empresas ficticias para la contratación de personas, el blanqueo de capital, el *hoax* –que son los mensajes engañosos en cadena– y el fraude de pago –es menos frecuente pero se dan, por ejemplo, cuando la gente paga por adelantado porque le dicen que ha ganado un premio y tiene que pagar cierta cantidad.

Con relación a ello, nos planteamos si es delito o no suplantar la identidad, aquí nos encontramos un vacío legal que vamos resolviendo por la vía penal y por la administrativa. Por ejemplo, en el caso de la creación de un perfil falso de un conocido personaje, lo probable es que la única opción que le quede al suplantado sea pedir a la red social que elimine ese perfil porque es falso o está siendo utilizado de forma fraudulenta.

Cuando en una suplantación se utilizan datos de carácter personal, entonces sí entramos en acción: en el artículo 7 de la Constitución Española, e incluso en el artículo 401 del Código Penal, se plantea la suplantación de estado civil y se citan penas de tres meses a tres años. ¿Qué ocurre? Que probar esa suplantación es muy complejo. Hay una sentencia del Tribunal Supremo que llega mucho más allá e indica que es necesario realizar algo que solo pueda hacer esa persona por su facultad, derechos y obligaciones, como puede ser el pago con una tarjeta de crédito. Distinto es cuando ese ataque o esa suplantación de identidad se hace con un acceso ilícito a una cuenta o correo, entonces sí que pasamos la barrera de lo ilícito y el aprovechamiento de esa cuenta puede llevarnos hasta un proceso judicial, y un delito de encubrimiento y revelación de secretos, según el artículo 127 y siguientes del Código Penal, o un delito de daños según el artículo 264.9.

En principio, podemos pensar que esto está perfectamente solucionado una vez trasmitido a las autoridades, pero puede suceder que una persona se haga pasar por otra y cuelgue una foto en Internet o haga, en su nombre, una serie de comentarios o de insultos e injurias relacionados con determinado colectivo. En un caso en que se daba esta situación, la Agencia Española de Protección de Datos ha resuelto en diciembre de 2011 como infracción grave.

Nosotros, en cuanto tenemos conocimiento de que es posible que se haya producido este tipo de delito, firmamos determinados protocolos tanto con proveedores del servicio como con intermediarios. Por ejemplo, con Tuenti, sin ir más lejos, tenemos un protocolo de coordinación en el que en el momento que sucede un incidente, según su importancia, se puede realizar un borrado de perfil, y además compartimos una serie de datos en espera de investigación. Es algo muy ágil, muy rápido.

La recomendación de las Fuerzas y Cuerpos de Seguridad del Estado es siempre la misma: sentido común, pero es uno el que debe ser responsable de sus propios actos.

¿Qué se puede hacer para gestionar bien la identidad en la red? La recomendación de las Fuerzas y Cuerpos de Seguridad del Estado es siempre la misma: sentido común. Los datos salen de uno mismo y uno debe decidir qué es lo que quiere compartir con los demás. Nosotros estamos ahí para velar porque cumplan y hacer cumplir la ley. Pero es uno el que debe ser responsable de sus propios actos. Cuando uno comparte una foto con un amigo y el amigo está en otros grupos de amigos, al final, es difícil evitar que la foto se propague por la Red.

8.4 Punto de vista de un operador de telecomunicación

Richard Benjamins
Telefónica Digital

Preguntas de las que partió su intervención:

- Para cualquier empresa, la correcta gestión de la relación con el cliente así como su profundo conocimiento se revelan como actividades básicas para el desarrollo del negocio. ¿Cómo está enfrentando este reto de *customer centric company* una operadora de telecomunicación como Telefónica?

Acerca de la identidad digital y sus consecuencias, querría exponer no tanto lo que está haciendo Telefónica hoy en día en el mercado sino cómo pensamos que tienen que cambiar las cosas, centrándonos sobre todo en el rastro digital que dejamos todos a lo largo de nuestra vida. En este sentido, se habla del *big data*: si una persona coge diez años de su vida, estos caben en pocos gigas. Hay gente que lo hace, que graba sus conversaciones, graba también sus fotos, sus llamadas, utiliza cámaras, de manera que después de diez años podrían tenerse 44 gigas de contenido.

Telefónica está haciendo una prueba con Bank of America sobre el tema del fraude porque una operadora móvil sabe exactamente cuándo alguien está en el extranjero puesto que el *roaming* deja un rastro. Si esos datos se los das a un banco, este sabe que esa persona está en el extranjero y, por lo tanto, todas las transacciones de esta persona en este país serán posiblemente ciertas. En España no existe esa costumbre por parte de los bancos pero, por ejemplo en Estados Unidos, debes avisar a tu banco si sales al extranjero. Este es un ejemplo del rastro que todo el mundo deja

y que aporta valor a la sociedad, al comercio... Telefónica ha decidido hace poco centrarse en estos rastros digitales que dejan todas las personas con el objetivo de convertir todos esos rastros en un activo nuevo. Se dice que los datos son como el nuevo petróleo, y el petróleo tiene una gran cantidad de utilidades positivas aunque también comporta riesgos, como sucedió en el golfo de México en Estados Unidos el año pasado. La pregunta es: «¿Estos datos son tan buenos para todos, o se pueden convertir en un riesgo?». Hace dos días hubo un evento en Barcelona con expertos de todo el mundo que trabajan en estas áreas y se constató que es un terreno muy interesante para muchos desarrollos. Se sabe que empresas como Google o Facebook guardan todos los datos de lo que está pasando.

Se dice que los datos son como el nuevo petróleo, y el petróleo tiene una gran cantidad de utilidades positivas aunque también comporta riesgos.

Los clientes de Google y Facebook no son sus usuarios del buscador o de la red social. Sus clientes son los anunciantes. Google y Facebook captan datos de usuarios para después hacer negocios con ello. Para los operadores captar los datos es un efecto complementario, el propósito no es guardar los datos, que es algo secundario, el propósito es establecer comunicaciones. Con cada vez más servicios digitales, las operadoras también recogen gran cantidad de datos muy valiosos. Por ejemplo, respecto a las *smart cities*, con todos los datos que tiene una operadora se podría hacer hoy una *smart city.* No hacen falta sensores en la calle, puesto que ya hay un sensor: el teléfono móvil, que dice exactamente dónde estás.

Los clientes de Google y Facebook no son sus usuarios del buscador o de la red social. Sus clientes son los anunciantes. Google y Facebook captan datos de usuarios para después hacer negocios con ello.

Las opiniones son divergentes: hay personas que afirman «Asúmelo, la privacidad ha muerto» y otras que advierten que hay que tener cuidado. Hoy, una operadora como Telefónica es como una persona en la cuerda floja: intenta buscar el equilibrio entre qué me dejan hacer y lo que quiero hacer. Mis clientes han depositado en mí su confianza y no puedo defraudarla. Toda esa cantidad de datos no será una realidad hasta que las propias personas digan «Por favor, usen mis datos para mejorar mi vida». Tus datos pueden decir si tienes riesgo de padecer cáncer, porque tus datos conocen por dónde va una persona, qué tipo de cosas hace y, estableciendo correlaciones, pueden sacarse conclusiones.

Ilustración 9. Richard Benjamins.

Los datos te informan sobre quiénes son tus mejores amigos y quiénes, tus colegas profesionales. Se han hecho pruebas sobre la identidad digital comportamental: si coges a las cinco personas a las que más llama una persona durante un largo período de tiempo, podrías identificar a esa persona al 90 %. Esto se debe a que cuando haces una llamada, deja un rastro. Si ese rastro se prolonga en el tiempo, define patrones que identifican a las personas que están más cerca a ti, son redes sociales, pero no aquellas en las que tú dices quién es tu amigo, sino que son redes sociales comportamentales. Si pierdes el pasaporte y acudes a la policía diciendo quiénes son las cinco personas con las que más hablas, hoy en día podrían identificarte sirviéndose de la tecnología. Aquí es donde surge la alarma. ¡Cuántas cosas saben de mí! Este es el tema clave en la actualidad en la economía digital. Hay muchos estudios sobre si a las personas les importa su privacidad y cuánto vale, pero si haces un estudio en el que quieres obtener un resultado, lo tendrás, depende de cómo hagas las preguntas. Un ayuntamiento de una localidad de Inglaterra ofrece la posibilidad de no cobrar impuestos a sus habitantes si estos consienten que sus datos sean utilizados para fines publicitarios.

Un ayuntamiento de una localidad de Inglaterra ofrece la posibilidad de no cobrar impuestos a sus habitantes si estos consienten que sus datos sean utilizados para fines publicitarios.

Paloma Llaneza: Los habitantes pueden estar contentos porque ignoran el alcance del consentimiento que han dado. Para cuando ya lo son y comienzan a ver los efectos de la cesión de sus datos, y la negativa repercusión que los mismos puedan tener, entonces empiezan las quejas sobre la legislación, la labor de las autoridades...

Juan Crespo: Con estos rastros que se dejan se están creando una serie de perfiles. Cuando queríamos demostrar que un delincuente estaba en un sitio determinado, hemos ido a hablar con el operador para conseguir datos sobre su localización y su rastro, con lo que se ha logrado demostrar que alguien había estado en un sitio determinado. No obstante, para poder hacerlo se ha pedido una orden judicial, dado que se violan una serie de derechos del ciudadano, o se está en la raya entre lo que se debe o no hacer. Yo, por ejemplo, tengo instalado un servicio que se llama Disconnect, el cual no permite al operador registrar lo que estoy haciendo. Con el DNI electrónico lo que se ha evitado es que se puedan crear perfiles, al separar la autoridad de validación de la de certificación. Así, sin que nadie lo pidiera y antes de que a alguien se le ocurriera pensar que la policía sabe todo lo que hace, se externalizaron los servicios de validación a otros sectores de la Administración, donde son manejados por personas que nunca sabrán de quién es el certificado que utilizan, ya que así se evita que se cree un perfil, de ahí que la policía nunca va a saber qué se hace con esos certificados porque no van a validarlos. Eso sí, todo se guarda, ya que si un ciudadano quiere saber qué se ha hecho con su DNI, hay que poder darles respuesta (también hay que dar respuesta a un juez, en caso de solicitarla). No obstante, se ha evitado que se puedan crear esos perfiles.

Richard Benjamins: Pero eso no tiene que ver con los datos. En Internet tienes muchos servicios gratis pero, a cambio, estás cediendo tus datos: así funciona la economía de Internet hoy en día. Nosotros creemos que no es sostenible, en algún momento pasará algo que dé la vuelta a todo, quizá llegue el regulador y diga: «Hasta aquí». Si la industria no se autorregula, van a pasar estas cosas.

Paloma Llaneza: Si yo me autorregulo y cometo una infracción contra mi autorregulación, ¿quién me sanciona? La autorregulación sin sanción no funciona, por lo tanto, la autorregulación, que es un concepto profundamente anglosajón, es un mecanismo del todo inválido, si saltarse la regulación no tiene consecuencias.

Richards Benjamins: Si quieres evitar cualquier abuso la autorregulación no funciona, pero a lo mejor funciona para el 90 % de los casos y hay que centrarse después en el 10 %, pero eso ya es una discusión política.

Paloma Llaneza: No es política, es legal. El concepto de autorregulación proviene de países con baja regulación legal y alta sanción indemnizatoria. En un país donde existe el daño punitivo como es Estados Unidos puede tener sentido la autorregulación como consenso empresarial y para evitar altas indemnizaciones ejemplarizantes, aunque si una empresa se comporta mal puede ser condenada a un daño patrimonial de 25 dólares y un daño punitivo de 25 millones de dólares. No obstante, en España y en Europa no tenemos el sistema de daño punitivo (solo existe el daño patrimonial y el moral) y para eso tenemos regulaciones extensas y profundas sobre casi todo con su sistema sancionador propio.

Richard Benjamins: Telefónica lo que está haciendo es intentar encontrar el equilibrio. Hay un proyecto llamado «Digital Confidence» donde el objetivo es empezar un viaje para ser transparente sobre qué datos tenemos en nuestra red, qué datos guardamos y por qué razón. Dar acceso al usuario a estos datos es lo que le permite actuar y tomar decisiones sobre ellos. El objetivo es cambiar la percepción, en vez de ver a las personas como víctimas de empresas que quieren usar sus datos personales, ponerlas en posición de control: que elijan a qué empresas cederlos y a cuáles no, es decir, el control es del usuario. Se está haciendo un piloto y en unos meses habrá una página web en O2, en el Reino Unido, que permita a los usuarios entrar y ver qué datos tenemos sobre cada uno de ellos. Se podrá, de esta manera, conocer la opinión de los mismos.

> El objetivo es empezar un viaje para ser transparente sobre qué datos tenemos en nuestra red, qué datos guardamos y por qué razón.

Hay una gran cantidad de *startups* que están trabajando directamente en este concepto, desde lo que está pasando ahora hasta mucho más allá, con una visión de largo plazo. Por ejemplo, una empresa como **Allow** permite que los usuarios le envíen sus propios datos, y ella se encarga de borrarlos de todas las bases de datos de publicidad, de manera que los datos de esos clientes son más escasos, por lo que valen más. Después, con los datos de sus clientes, va a hablar con grandes compañías para tratar de vender esta información, y un 70 % del dinero que se recauda se destina a los propios usuarios. Es un modelo como el de Google pero invertido, de repente el usuario es el que cobra por sus datos personales. Hoy en día cuentan con unos treinta mil usuarios y nadie sabe si esto va a crecer o no, pero hay un gran interés.

> Es un modelo como el de Google pero invertido, de repente el usuario es el que cobra por sus datos personales.

Algunas empresas tienen un enfoque como extensión al antivirus, el problema ya no está solo en tu ordenador, está en la red: qué dice la gente de ti. Reputation.com ha conseguido bastantes clientes de profesiones liberales (cirujanos, abogados...). La empresa hace un rastreo de toda la web, de las redes sociales... y elabora un informe sobre lo que se dice de ti, si es positivo o negativo... El informe se envía semanal o mensualmente y tú decides lo que quieres que se elimine. Algunas cosas no se pueden quitar sin la colaboración de la web que publica los datos; en otros casos se pueden utilizar técnicas de SEO para bajar su posición y que no salga en las búsquedas. Este es un modelo de negocio que antes no existía. En Alemania hay una empresa que hace exactamente lo mismo pero para proteger a los niños. Es un servicio que contratan los padres para que rastreen las redes sociales y elaboren un informe que te dice con quién habla tu hijo, cómo son esas personas con las que habla a juicio de la empresa... Esto sirve para mejorar la sociedad, es un modelo de negocio distinto y veremos si tiene éxito o no.

Juan Crespo: Vosotros tenéis un servicio de reputación que se puede contratar y se dedica a mirar en Internet qué se dice de las empresas y se elaboran informes, según el tipo de contrato que se haga, sobre qué se dice de una determinada empresa en ese momento.

Richard Benjamins: Sí, pero aquí hablamos de algo que va un poco más allá: no solo te lo cuentan sino que actúan en consecuencia. En una visión a más largo plazo hay empresas tipo **personal.com**, una web estadounidense que guarda por ti algunos de tus datos personales. Así, por ejemplo, si esta empresa tiene los datos de tus seguros (de casa, coche...) te permitirá acceder a través de tecnologías seguras a portales relacionados, por ejemplo, a aseguradoras para que te hagan ofertas mejores que las que tienen normalmente. Son servicios muy personalizados basados en los datos de cada uno.

Si esto que aún es incipiente se desarrolla en un futuro, al final de tu vida tú, tus hijos, tendréis todos los datos de vuestra vida en un único sitio. ¿Qué pasa con tus datos cuando falleces? Hay muchas discusiones en torno a cuál es la mejor entidad para que asuma la función de guardar por ti esos datos, ¿es el Estado?, ¿es un banco?, ¿es una operadora?

Hay que ver los datos como una propiedad nuestra, y a quién podemos dejárselos, igual que dejamos nuestro dinero a un banco o a otra entidad.

Hay que ver los datos como una propiedad nuestra, y a quién podemos dejárselos, igual que dejamos nuestro dinero a un banco o a otra entidad. El usuario puede ceder su uso para distintos fines: por ejemplo, los datos de localización se pueden ceder para que los utilice el Ayuntamiento para optimizar el tráfico, los datos médicos se pueden ceder en beneficio de la investigación. A cambio, el usuario podría, por ejemplo, obtener descuento en la Seguridad Social, en los impuestos de basura... Hay muchas cosas por explorar, y si nadie se atreve a hacerlo no va a pasar nada. Afortunadamente, ahora hay una gran cantidad de empresas *startups* que están consiguiendo dinero para invertir en este campo.

Paloma Llaneza: Principalmente en Estados Unidos ya que el entorno regulatorio es propicio. Además, el símil con el dinero no es un buen ejemplo porque los datos son replicables de manera infinita y no se sabe dónde pueden acabar. Soy consciente de cuándo mi dinero sale de mi cuenta, pero no de cuándo se duplican mis datos.

Richard Benjamins: Hoy no, pero quizá algún día se haga un extracto cuando alguien use tus datos.

Paloma Llaneza: Quizá pueda haber un informe de los dos primeros escalones, pero de los demás lo dudo, es muy difícil.

Richard Benjamins: Hoy en día con los datos que tenemos de cómo funciona no podríamos hacerlo. No obstante, se trata de cambiar el chip de cómo pensamos, y yo creo que es nuestra obligación hacerlo.

8.5 Punto de vista tecnológico

José María del Álamo
Universidad Politécnica de Madrid

Preguntas de las que partió su intervención:

- La creciente actividad en la Red de las personas está haciendo necesaria la gestión de la identidad digital de una manera cada vez más activa. ¿De qué herramientas disponemos actualmente para hacerlo de un modo efectivo? ¿Qué retos tecnológicos se plantean para llevarlo a cabo?

En relación con lo último que ha comentado Richard sobre la reputación, existe la tentación de inundar la Red con información positiva para que la negativa caiga en los buscadores y sea más difícil de encontrar. Sin embargo, esto puede crear otro problema: no saber si toda esa nueva información es cierta o falsa. Técnicamente es una solución a un problema existente, aunque puede que no sea la mejor. Respecto a las tendencias que se han comentado, parece que está produciéndose una transformación de la intimidad y la privacidad y eso afecta a cómo se gestiona tecnológicamente la identidad. Respecto a los modelos de negocio centrados en el usuario, tradicionalmente se utilizaba el CRM (*customer relationship management*), es decir, la gestión de las relaciones con los clientes, pero también existe la versión complementaria que es VRM (*vendor relationship management*) o gestión de la relación de un usuario con vendedores: desde el punto de vista del usuario, si tienes la información puedes gestionarla de la forma más adecuada para ti y ofrecérsela a quien esté interesado en ella. Ya hay empresas que están ofreciendo estas soluciones VRM de manera comercial.

> Está produciéndose una transformación de la intimidad y la privacidad y eso afecta a cómo se gestiona tecnológicamente la identidad.

Respecto a la persistencia de la información: las palabras se van pero lo que está escrito se queda, y mucho más en el mundo digital. Antes, cuando algo quedaba escrito en un libro, tenías que ir a la biblioteca, saber qué libro era... Ahora una simple búsqueda te puede ofrecer muchísima información al instante. Se habla del derecho al olvido y, aunque técnicamente es complicado, puede no ser imposible porque existen, por ejemplo, mecanismos de cifrado por los que se podría ocultar toda la información de uno mismo (tecnologías como el DNI electrónico). ¿Es eso económicamente viable e incluso conveniente? Eso es más discutible, puesto que el trabajo que debe realizarse y el volumen de datos que ha de manejarse parecen no escalar.

> Las palabras se van pero lo que está escrito se queda, y mucho más en el mundo digital.

Hay una componente social que afecta bastante al derecho al olvido: las redes sociales. Estas surgen a partir del año 2000 y están orientadas principalmente a una generación de adolescentes que tienden a publicar la información, por lo que hacen de altavoces. Con anterioridad, los adolescentes hacían esto en su grupo de amigos pero ahora lo hacen en lo que creen que es su grupo de amigos en Facebook. Sin embargo, ya no lo ven solo los grupos de amigos, sino que esa información es diseminada sin mucho control. Es más, la tecnología permite conseguir interfaces para el acceso a esa información de forma automática: Facebook, por ejemplo, dispone de interfaces para realizar consultas y obtener datos de una persona. A día de hoy, se requiere autorización de esa persona.

Las tecnologías existentes para delegación de la identidad del usuario posibilitan integrar la vida e identidad social de la persona en el resto de la web.

Las tecnologías existentes para delegación de la identidad del usuario posibilitan integrar la vida e identidad social de la persona en el resto de la web. Con el «Me gusta» de Facebook firmamos que algo nos ha gustado, y esa información se asocia semánticamente al perfil de usuario en la red social de manera automática. Por lo tanto, ya estás ligado para siempre a esa información. También se pueden hacer comentarios y comentar una página con tu perfil de Facebook. Con ello, esa información queda asociada al perfil de Facebook con doble vertiente: por un lado, que se publica en Facebook y se traslada a todos los contactos; por otro, esa información queda asociada a tu identidad en el sitio donde se ha introducido el comentario.

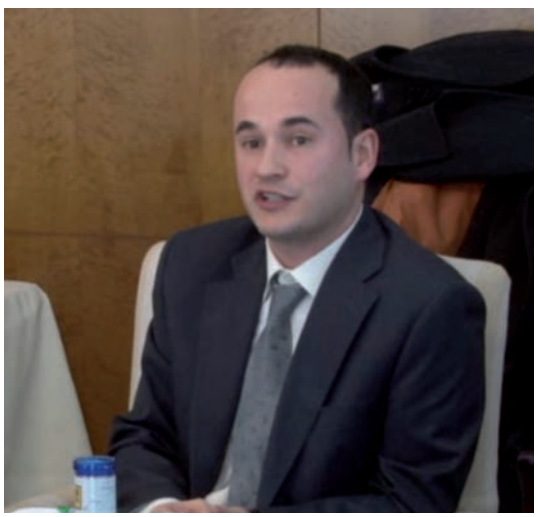


Ilustración 10. José María del Álamo.

Se está avanzado en el derecho a la réplica, es decir, la posibilidad de que cuando alguien encuentre una información antigua encuentre también la nueva.

Hay casos en los que, una vez hecho un comentario, se puede cambiar de opinión (la opinión humana evoluciona igual que nuestra mentalidad). Se puede intentar inundar la red con esa nueva información mencionada con anterioridad pero es técnicamente muy difícil. Se está investigando y se está avanzado en el derecho a la réplica, es decir, la posibilidad de que cuando alguien encuentre una información antigua encuentre también la nueva, lo cual sería muy útil. Hoy en día existen soluciones legales, aunque son complicadas, contra la difamación por ejemplo. No obstante, es un proceso muy largo y lento y tal vez lo que se consiga sea el efecto contrario: que se llame la atención sobre aquello que no quieres que la gente conozca. Quizá sería más sencillo intentar superponer o añadir esa información nueva a aquella que no te conviene porque, además, hay veces que no entra en el terreno de lo que es legal o no.

Hasta ahora el problema de la privacidad se centraba sobre la información que yo emito y difundo al resto del mundo, pero estamos empezando a ver que no solo yo emito información sobre mí, sino que hay mucha gente que habla sobre mí, que añade comentarios, que me cita o enlaza a mi perfil en cualquier red social o correo electrónico, y esa información queda de forma persistente. Aunque no lo publique uno mismo, eso también afecta a su privacidad y derivadas de la misma, como es la reputación. Aunque a los adolescentes que en su momento entraron en Facebook no les afectaba mucho, ahora les empieza a afectar: según va pasando el tiempo adquieren poder adquisitivo, puestos de responsabilidad en empresas...

Richard Benjamins: No lo sabemos.

José María del Álamo: Se sabe, por ejemplo, que las herramientas de reputación están en auge y puede que no en cualquier contexto, pero en nichos específicos, si vas a contratar a alguien de alta dirección, sí se tiene en cuenta.

Richard Benjamins: La generación Facebook va a crecer y los presidentes de los países formarán parte de esa generación.

Paloma Llaneza: Yo creo que lo sabemos ya: cuando nos convertimos en padres olvidamos al joven que fuimos y los errores que cometimos, y pasamos a exigir a nuestros hijos en función de nuestro punto de vista de la madurez. Lo mismo pasará con los errores de juventud en las redes sociales, que se tratarán con la misma dureza con la que los padres ven los errores de sus hijos.

Juan Crespo: Antes has comentado una cita, y hay otra básica: «Yo soy yo y mis circunstancias». Las circunstancias de la identidad digital son impredecibles.

Ruth Gamero (Telefónica I+D): Hay que distinguir entre lo que es identidad y lo que es privacidad. Sí es verdad que la privacidad está cambiando y no nos importa contar en un círculo cada vez más amplio lo que hacemos en nuestra vida personal. Sin embargo, puedo estar interesado en que una cosa que creo que está mal no la sepa el resto de la gente –sería lo que se denomina la «mancha del honor»–, ya que nuestra identidad es nuestra reputación y la gente se va a preocupar de protegerla.

Nuestra identidad es nuestra reputación y la gente se va a preocupar de protegerla.

Paloma Llaneza: Habría que distinguir dos tipos de circunstancias: las personales y las sociales. Por ejemplo, una persona cuando adquiere un puesto de relevancia puede arrepentirse de comentarios que ha realizado en redes sociales e incluso puede aparecer un problema de seguridad. En caso de cambio de régimen político, una circunstancia personal que podía estar bien vista o legalmente aceptada se puede convertir en un lastre o un serio problema legal para toda tu vida.

8.6 Punto de vista de experto en análisis de datos

Jesús Cid
Universidad Carlos III de Madrid

Preguntas de las que partió su intervención:

- Una de las ventajas de disponer de ingentes datos sobre la actividad de las personas en la Red es la de poder analizar el comportamiento, los gustos y el uso que se hace de los servicios. ¿Qué posibilidades nos ofrece la tecnología para utilizar esta información en vías de mejorar la toma de decisiones? ¿Y cuáles son los principales retos tecnológicos en este sentido?

La minería de datos tiene interés por la cantidad de datos de que disponemos, y el enorme reto que plantea su gestión y procesamiento a gran escala. Aunque este problema no es nuevo, empieza a ser nueva la escala a la que crece la dimensión de los datos y la universalidad del acceso a los mismos.

Empieza a ser nueva la escala a la que crece la dimensión de los datos y la universalidad del acceso a los mismos.

Ya no es solo un problema de grandes compañías como Google o Visa, sino que la disponibilidad de grandes volúmenes de información está al alcance de empresas más pequeñas. Comienzan a surgir soluciones tecnológicas que pretenden dar posibilidades de computación masivamente paralela, de redes de ordenadores, de servicios de cómputo y almacenamiento... Con estas tecnologías, los propios datos adquieren valor, y existe la posibilidad de comprarlos. En suma, empresas de tamaño más pequeño podrán también hacer minería con grandes volúmenes de información y quizá la tendencia va a ser que la aplicación de técnicas de acceso a la minería esté más generalizada.

El reto es cómo pueden las organizaciones o empresas sacar información que pueda ser útil para predecir el comportamiento, conocer los gustos o identificar las preferencias de los usuarios.

El objeto de la minería es extraer información, sacar valor de los datos. La importancia radica en conseguir predecir u obtener información útil con los datos que se tienen. En el ámbito de la identidad digital y del uso de la información personal que tienen las empresas, el reto es cómo pueden las organizaciones o empresas sacar de ahí información que pueda ser útil para predecir el comportamiento, conocer los gustos o identificar las preferencias de los usuarios. Como siempre, se puede hacer para bien o para mal, pero la parte positiva sería que aquellos que conocen nuestras preferencias nos pueden ofrecer mejor aquello que más nos interesa. Con este fin han surgido los sistemas de recomendación que intentan, a partir de la información de los usuarios, predecir qué les va a interesar y qué no. Aquí entrarían también las redes sociales. Hay una manera que parece obvia de hacer una recomendación a un usuario: consiste en preguntarle qué le gusta, que te lo responda y mirar qué características presentan los productos que tengo para ver cuáles son los que más le pueden interesar. En cambio, los sistemas de recomendación más conocidos, como los de Amazon, han utilizado otras técnicas que aprovechan, precisamente, la gran cantidad de información que hay sobre el historial de qué otras cosas han comprado los usuarios, y qué otras cosas han comprado usuarios parecidos. Existe un gran potencial de usar no solo información personal, sino también contextualizada con la de otros usuarios. Ese es el gran valor que tiene disponer de toda esa información conjunta y agregada. De hecho, los sistemas de recomendación que han empezado a funcionar un poco mejor han ido por esa línea, estudiando si ese producto interesó a otros usuarios con un perfil parecido o si productos similares interesaron a ese usuario en el pasado, para construir grandes matrices de intereses de usuarios y productos y a partir de ahí hacer inferencias.

Existe un gran potencial de usar no solo información personal, sino también contextualizada con la de otros usuarios.

La aparición de grandes volúmenes de datos nos da información acerca de las conexiones entre usuarios, de ahí el gran valor de la información de redes sociales. También da muchas pistas sobre el comportamiento que van a tener los usuarios ante la suscripción de un servicio; por ejemplo, si un usuario se da de baja de Telefónica, hay cierta probabilidad de que esa baja se propague a través de su red social, es decir, que conocidos suyos adopten actitudes parecidas.

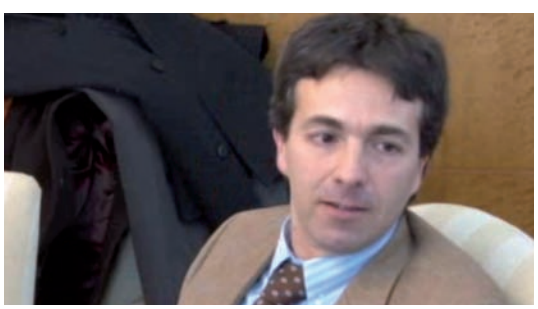


Ilustración 11. Jesús Cid.

También tiene mucha importancia la privacidad. Uno de los sistemas de recomendación más conocido es el de Netflix. En el año 2006, este servidor de vídeos organizó un concurso que premiaba con un millón de dólares a quien encontrara un sistema de recomendación que mejorara las prestaciones del que ellos tenían. Netflix publicó un 10 % de su base de datos y para proteger la privacidad borraron el nombre de los usuarios. Sin embargo, posteriormente hubo quien fue capaz de inferir a partir de los perfiles, comparándolos con rastros de esos usuarios en otros sistemas, los nombres de los usuarios. Esto nos muestra lo difícil que es proteger la privacidad en estos casos.

Sobre el tema de la identificación de gustos e intereses de los usuarios, hay mucho potencial en las tecnologías para ayudarnos a interpretar el contenido de forma automática (*content understanding*). Este es el problema más difícil: sacar contenido semántico de los datos, de una fotografía, de una imagen, de un vídeo... En los próximos años veremos mucho progreso en las tecnologías de interpretación de imágenes o interpretación a más alto nivel del contenido, ya existen sistemas que permiten identificar caras bastante bien. Ayuda mucho el entusiasmo de la gente por etiquetar el contenido, por ejemplo en Facebook, porque permite entrenar máquinas para que sean capaces de identificar a personas en fotografías.

En los próximos años veremos mucho progreso en las tecnologías de interpretación de imágenes o interpretación a más alto nivel del contenido.

Yod Samuel Martín (experto de la Universidad Politécnica): La automatización de este tipo de actividades conlleva ciertos peligros; por ejemplo, en ocasiones las personas etiquetan fotografías con nombres de personas que no aparecen en ellas. Incluso en Estados Unidos hay aplicaciones que infieren la tendencia política de un usuario en función de los amigos con los que esté relacionado, ante lo cual hay también un servicio que te permite añadir perfiles falsos de amigos de otras ideologías.

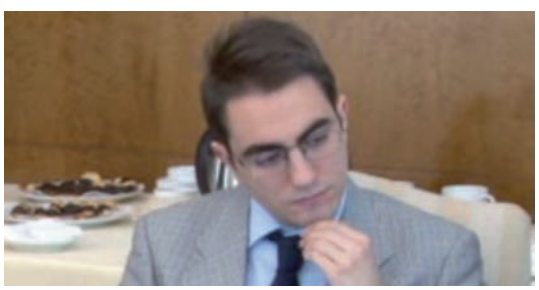


Ilustración 12. Yod Samuel Martín.

Antonio Castillo: Un ejemplo de minería de datos de una empresa española fue un servicio realizado para el periódico *Marca* que, en función de los resultados de la jornada, era capaz de inferir el número de periódicos que iban a venderse en cada quiosco, además con un elevado grado de acierto. También ha habido aplicaciones que permitían prever las zonas en las que es más posible que se produzcan problemas de delincuencia en función de una serie de datos.

Juan Crespo: La policía tiene una unidad de ámbito nacional llamada Unidad de Inteligencia Criminal. El año pasado se presentó la Unidad de Análisis de Conducta, que trata de recabar información sobre hechos delictivos para poder determinar patrones en las conductas de los delincuentes.

8.7 Punto de vista de la legislación-regulación

Paloma Llaneza
Abogada. Autora. Bloguera. Lectora

Preguntas de las que partió su intervención:

- En un entorno en el que ofrecer datos de carácter personal como medio para acceder a servicios en la Red de manera gratuita es algo habitual, ¿es posible asegurar la protección de los derechos fundamentales de los ciudadanos? ¿Podemos confiar en entidades privadas que prestan servicios en todo el mundo pero que mantienen su domicilio en un Estado concreto para que respeten nuestros derechos y defiendan nuestras libertades?

Se puede hablar de dos grandes áreas: quiénes creemos que somos y quiénes somos en realidad. Habría una tercera área que sería quiénes creen los demás que somos.

En primer término voy a hacer una especie de manifestación pública de mi identidad: soy lacaniana, castellana, abogado y ciudadana. Estos cuatro elementos de mi identidad mediatizan lo que voy a decir, porque obviamente todos venimos mediatizados por un entorno. Cuando digo que soy lacaniana quiero decir que mantengo, como Lacan, que el ser humano no cambia a partir de los tres años, por ello, no creo eso de que las redes sociales nos cambian. Lo único que hacen las redes sociales es potenciar algunos aspectos de nuestro carácter o enseñarnos los comportamientos con una base. Todo depende de lo que es la identidad: si estamos hablando del núcleo de la identidad, de lo que somos en lo más profundo de nuestro ser, o si estamos hablando desde un punto de vista más amplio de identidad que sí que puede cambiar, nuestros gustos evolucionan.

Ilustración 13. Paloma Llaneza.

Fundamentalmente se puede hablar de dos grandes áreas: quiénes creemos que somos y quiénes somos en realidad. Habría una tercera área que sería quiénes creen los demás que somos, que es la reputación que se forma con una gran subjetividad, dado que los demás están influidos por todos sus filtros personales cuando te miran. Por lo tanto, la imagen que tú

reflejas en el espejo de cada una de las personas que te miran es distinta, de ahí que la reputación sea tan inmanejable.

La imagen que tú reflejas en el espejo de cada una de las personas que te miran es distinta, de ahí que la reputación sea tan inmanejable.

Yod Samuel Martín: En psicología se habla de la ventana de Johari, los cuatro cuadrantes en los que se divide la personalidad según lo que nosotros conocemos y lo que conocen los demás. Aparecen, por consiguiente, cuatro cuadrantes, lo que yo no conozco y conocen los demás se llama el punto ciego. Aquí aparece otro plano que es lo que los demás dicen de mí.

Paloma Llaneza: Ese plano ha existido siempre, por eso son tan actuales las citas de Lope de Vega sobre la honra. El concepto de honra del Siglo de Oro vuelve con toda su pujanza. Como todo esto es muy difícil de manejar, yo me he ido a la criptografía. La criptografía para identificarte utiliza lo que tienes o lo que eres, lo que sabes, y yo añado también una capa, que es lo que hacemos. Para intentar conceptualizar esto, he hecho dos grandes áreas.

La primera es la de la identificación y autenticación, o quién eres. En este caso, yo no puedo decir que soy yo, necesito una tercera parte que tiene que ser de confianza para que me identifique. Un reflejo de esta área sería el anonimato: el derecho a ser anónimo. Cuando una persona paga en efectivo nadie sabe lo que está comprando y se mantiene en un anonimato. Ello entra en conflicto con el derecho de las sociedades de protegerse ante personas que delinquen. Es un equilibrio entre derechos fundamentales y orden público.

Yo no puedo decir que soy yo, necesito una tercera parte que tiene que ser de confianza para que me identifique.

La otra área sería la huella digital o lo que hacemos, que podemos hacerlo identificados o sin identificar, ese *link* entre esas dos entidades es de donde surge todo este debate. Sobre los datos anónimos la legislación no tiene nada que decir (datos agregados y estadísticos), es respetuosa al respecto puesto que entiende que reflejan cómo el ser humano se comporta y estos datos pueden ser usados para bien o para mal. Se podrán seguir agregando datos de la gente siempre y cuando se sea capaz de mantener en el anonimato a quiénes están produciendo esos datos. El problema es cuando se produce un *link* entre la identificación y la acción, ya que se está atribuyendo una actuación a una persona en concreto. A partir de ahí también está la cuestión de la robustez de la identificación: si me han identificado correctamente, todo lo que haga me será atribuible legalmente para bien o para mal, desde firmar un contrato hasta cometer un delito.

Lo que ocurre, y es el siguiente paso, es que aquí tiene que haber un negocio, la diferencia estriba en que cuando yo pago por llamar por teléfono espero que respeten mis datos, pero cuando entro en Facebook, si no hay producto, el producto claramente soy yo, producto del que Facebook se alimenta para vender los datos a quien sea. Pero, además, existe el problema añadido de que ceden esos datos a las jurisdicciones en las que están. En Estados Unidos está la USA Patriot Act que permite al gobierno de ese país entrar en todas las bases de datos: si tienes acceso a una base de datos como la de Facebook, ya no necesitas una agencia de investigación. Es muy preocupante que toda esa información esté al alcance de un Estado al que se puede ir de visita. Recientemente se han introducido nuevas cláusulas en Google que permiten realizar una minería de datos para perfilar a sus usuarios, lo que puede contravenir algunas normas europeas como proporcionalidad del dato, consentimiento por servicio... Muchos modelos de negocio florecientes en Estados Unidos, con una legislación mucho más laxa, casi inexistente, no tienen cabida en Europa, y hay que tener en cuenta el impacto regulatorio porque en Europa es altamente limitante.

Cuando entro en Facebook, si no hay producto, el producto claramente soy yo.

No creo que el concepto de privacidad o el de intimidad hayan cambiado: la gente sigue llegando a los despachos de abogados quejándose de suplantaciones de identidad en redes sociales, de que han recibido críticas en un blog...

Antonio Castillo: En nombre de Fundación Telefónica os agradecemos vuestra intervención, el tiempo dedicado y haber compartido este rato tan agradable con nosotros.

Ilustración 14. Antonio Castillo.

Anexo

Tecnologías para la gestión de la identidad digital

En este apartado se hace una descripción de las diferentes tecnologías y tipos de herramientas que facilitan la protección de la identidad digital. Estas tecnologías tratan, por un lado, de ofrecer soporte al derecho a la intimidad y, por lo tanto, a mantener ciertos datos en la privacidad, y por otro, tratan de gestionar la identidad digital de una manera sencilla.

A.1 Herramientas para mantener la identidad del usuario de manera anónima

Cada vez existe una conciencia mayor de que las acciones que se realizan de manera cotidiana en la Red dejan un rastro que revela a terceros distintas porciones de la identidad digital. Crear un perfil social, escribir un comentario, navegar, etc. son tareas con las que se hacen públicos rasgos diferentes que forman parte de la identidad digital.

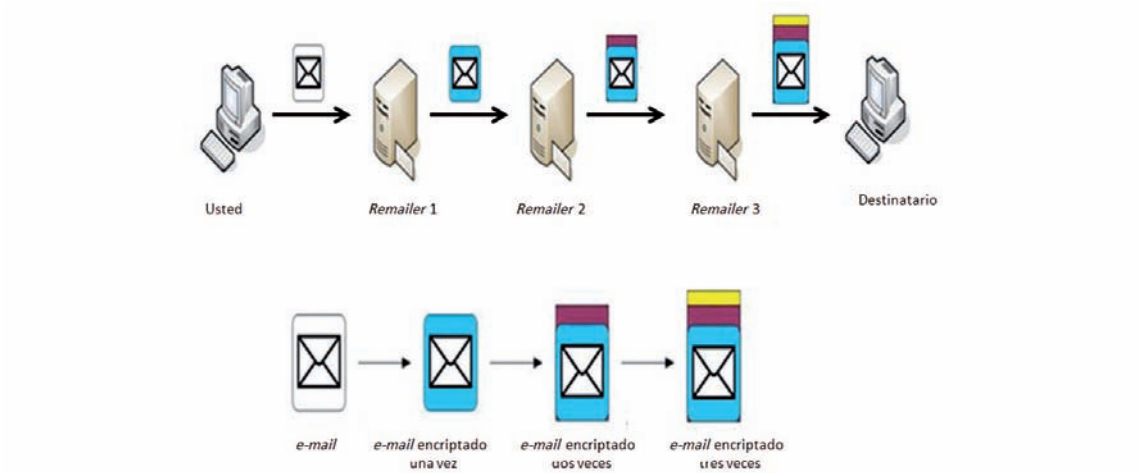
En este apartado se incluyen aquellas tecnologías y herramientas que facilitan al usuario la navegación anónima por la Red al mismo tiempo que le permiten no revelar datos en exceso o revelar solo los datos estrictamente necesarios para usar los servicios en la Red. Con estas herramientas se trata de proteger el derecho a la intimidad y de llevar a cabo una gestión preventiva de la identidad digital.

A continuación y de manera no exhaustiva se enumeran algunas de las soluciones más comunes en esta línea.

A.1.1 Herramientas para proteger la identidad digital en los *e-mails*

Las herramientas que sirven para proteger la identidad digital en los correos electrónicos también se conocen como *remailers* y existen varios tipos: en los de tipo 0 el *e-mail* va desde el usuario que lo envía hasta el *remailer*, que omite la identidad del usuario y lo envía al destinatario. Los *remailer* tipo 1 están basados en el mismo principio, pero con un número de mejoras como «encadenamientos» (usando cadenas de *remailers* independientes) y encriptación (figura 48). Los de tipo 2 hacen frente a problemas de seguridad de los *remailers* de tipo 1 modificando ciertos aspectos, como por ejemplo la fijación del tamaño de los mensajes y el envío de estos por separado. Finalmente, los *remailers* tipo 3 incorporan mejoras para manejar las respuestas a mensajes anónimos y la protección frente a ataques.

Figura 48. Ejemplo de *remailers* tipo 1



Fuente: Wikipedia.

A.1.2 Herramientas para proteger la identidad digital cuando se accede a servicios interactivos

Muchos servicios interactivos de Internet rastrean datos de los usuarios. De hecho, muchas webs de gran popularidad hospedan, de media, 65 rastreadores de terceros que permiten caracterizar a los usuarios en función de sus comportamientos de navegación. Por ello, se han desarrollado diferentes soluciones que permiten evitar este seguimiento y que, por lo tanto, aseguran la privacidad del usuario.

Entre ellas destacan Anonymizer.com y Onion Routing, herramienta que permite la navegación anónima creando un camino a través de diferentes Onion Routers, por donde se entrega la información de forma anónima. Otro ejemplo es The Freedom Network, un proyecto comercial (de pago) basado en el sistema PipeNet que incorpora algunas ideas del proyecto Onion Routing. The Freedom Network permite a los usuarios asignar un seudónimo persistente mientras se están comunicando a través de Internet. Sin embargo, el coste del mantenimiento del sistema era muy grande para los operadores ya que necesitaban todo un sistema mundial de Proxies Anónimos en Internet (nodos AIP), de modo que como el número de usuarios de pago no soportaba el sistema, este fue desechado.

Otros ejemplos son los Java Anon Proxy, un proyecto técnico de la Universidad de Dresden que funciona en Webs y Tor,[39] la evolución del Onion Routing project y que actualmente es la herramienta interactiva de anonimato de mayor éxito con varios cientos de miles de usuarios.

39. https://www.torproject.org/

A.1.3 Herramientas que minimizan la información que facilitan los usuarios en la Red

Otro conjunto de herramientas que permiten esta gestión adecuada de la información de los usuarios en la Red son las tarjetas de identidad o InfoCards.

A.1.3.1 U-Prove

Entre las tarjetas de identidad hay que destacar U-Prove, la solución de Microsoft (evolución de su anterior CardSpace) que provee de seguridad a todos los agentes en un sistema de identidad digital, incorporando tecnologías de criptografía, y que soporta las evoluciones de los servicios de la nube.

Los agentes de U-Prove son el software que hace de intermediario para separar el proceso de extracción de información de los proveedores de identidad de la publicación en un agente de confianza ayudando así al usuario a proteger su privacidad. Los agentes de U-Prove existen explícitamente para representar los intereses de los usuarios eligiendo compartir (o no) su información personal con webs en Internet.

Los agentes U-Prove están compuestos de un servicio en la nube y componentes opcionales de cliente local. El servicio de *cloud* puede ser usado por los principales navegadores para Windows y MacOS y la mayoría de los *smartphones*. En resumen, U-Prove usa códigos de encriptación para la transmisión de información (*tokens*) y dispone de un sistema en la nube para intermediar entre los proveedores de identidad y los agentes de confianza sin que la información pase por el equipo del usuario.

Para entender bien cómo funcionan estas herramientas, a continuación se describe un ejemplo: se trata de un escenario en el que hay que verificar ciertos campos de identidad en un agente de confianza, por ejemplo, en el caso de que una persona quiera vender su coche a través de Internet en una página de compra-venta, pero no queriendo revelar más datos de los necesarios (sin embargo, sí que quiere demostrar que es el propietario del vehículo y que dicho vehículo está a la orden de todos los pagos de impuestos, multas, etc.) (figura 49).

Figura 49. Funcionamiento de U-Prove en un proceso de compraventa

Fuente: Elaboración propia.

El esquema de funcionamiento podría ser el siguiente: el usuario estaría dado de alta en el agente de confianza (la página donde quiere vender su coche) y comenzaría el proceso de creación del anuncio. En este proceso la página le ofrecería la posibilidad de mostrar información verificada sobre la propiedad del vehículo, etc., y él la aceptaría sabiendo que esta información le dará credibilidad al anuncio y, por tanto, venderá el coche con mayor facilidad (paso 1).

La página de venta de coches a su vez puede tener una lista de proveedores de información verificada en los que confía. Esta lista se envía al agente U-Prove (paso 2) que se lo muestra al usuario, quien elige cuál de los proveedores puede ofrecerle la información (paso 3). En el caso bajo estudio puede ser el Departamento de Tráfico.

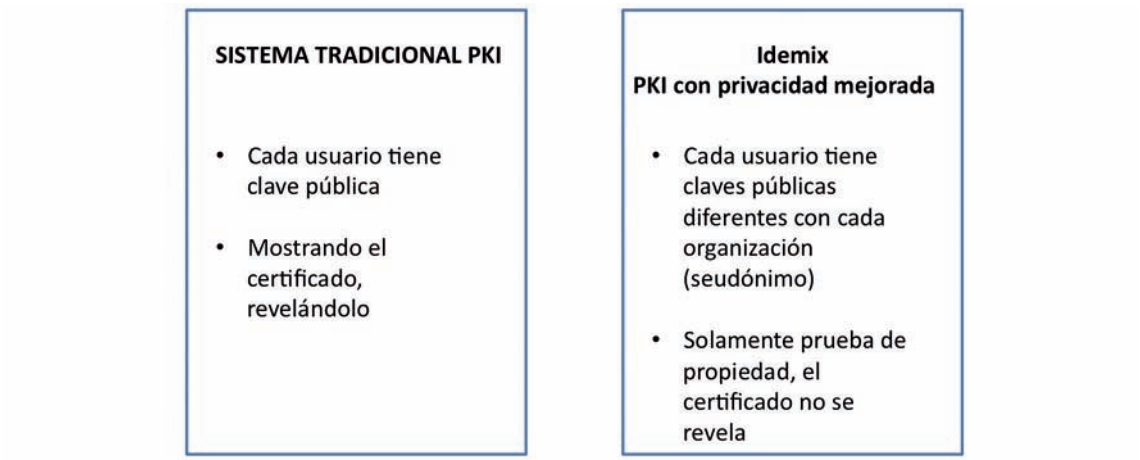
Una vez seleccionado el proveedor de información, se le redirige al sitio donde tendrá que autenticarse (paso 4). Una vez autenticado, el proveedor de identidad y el agente U-Prove del usuario crean los *tokens* (paso 5) que contienen los campos de información como el nombre, marca del coche, permiso de circulación, etc.

El agente U-Prove crea una presentación de los *tokens* que sean necesarios para el agente de confianza y se los manda (paso 6). Con estos datos, la página donde el usuario quiere vender su coche refleja información correcta y de una fuente fiable.

A.1.3.2 Idemix (ID Mixer)

Desde hace años los sistemas basados en PKI (Public Key Infrastructure) han sido utilizados para garantizar la identidad de transacciones en la Red. El sistema Idemix, de IBM, viene a suponer una mejora en cuanto a la privacidad de esta infraestructura, e incluye ciertas características para garantizar la privacidad, como se muestran en la figura 50.

Figura 50. Diferencias entre PKI tradicional e Idemix



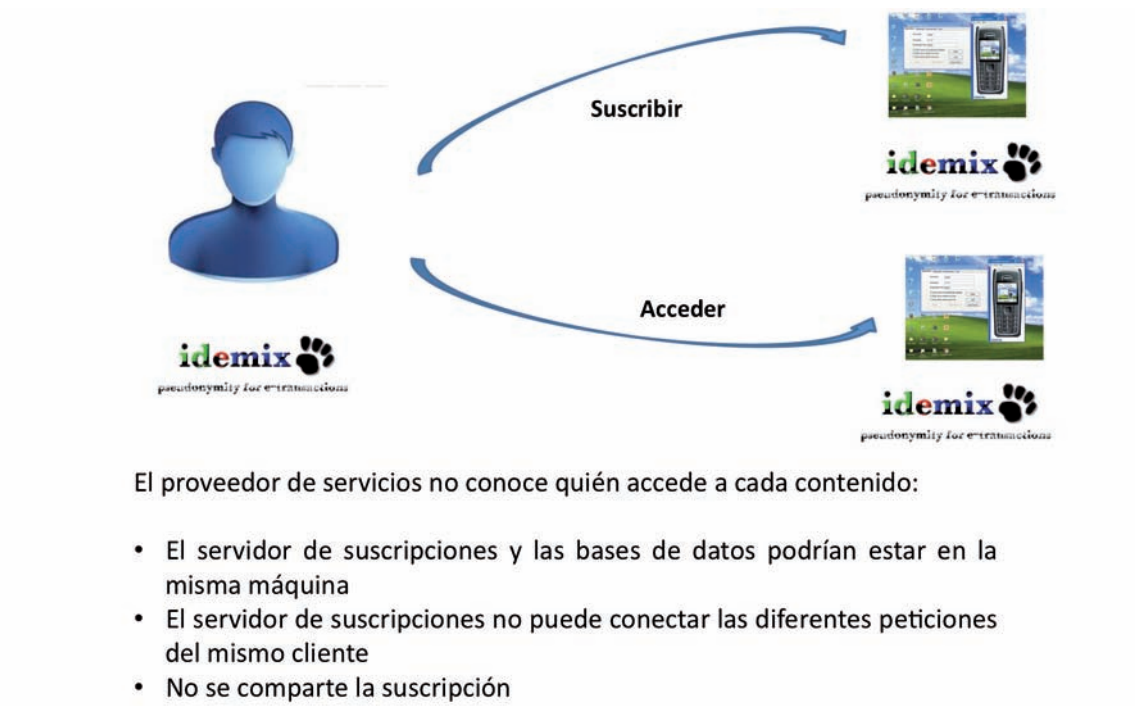
Fuente: Elaboración propia.

Idemix permite, por tanto, mantener la dualidad entre autenticación y privacidad. Gracias a su sistema de credenciales anónimas, se pueden seleccionar los datos de una identidad digital que se revelan. Así, a través de Idemix los usuarios obtienen del emisor una credencial con todos los datos de los que el emisor puede dar fe. Posteriormente, cuando un usuario quiere autenticarse ante un proveedor de servicios utiliza Idemix para transformar la credencial creada anteriormente en otra exclusiva para esta autenticación. La nueva credencial solo contendrá la información requerida para esta autenticación, sin aportar más datos de los necesarios. El usuario podrá realizar este proceso tantas veces como quiera, y las credenciales resultantes no podrán vincularse entre sí. De esta manera, un usuario podrá, por ejemplo, revelar su edad a la hora de acceder a un servicio que requiera la mayoría de edad pero sin revelar su nombre y, a continuación, hacer uso de otro servicio en que revele su nombre y no su edad, sin que ambas peticiones se vinculen, es decir, sin permitir que se conozca tanto su nombre como su edad. Esto garantiza que se mantenga el anonimato en los procesos en los que el usuario interacciona con los proveedores de servicios.

A continuación se muestran tres casos de uso explicando cómo se mantiene el anonimato:

- **Proceso de suscripción**: El usuario compra la suscripción *online* y recibe una credencial Idemix como recibo, durante esta transacción la identidad de cliente es conocida por el proveedor de servicios. A partir de entonces, cuando el usuario quiere acceder al servicio, utiliza un canal anónimo, prueba la propiedad de una credencial y se le concede el acceso al servicio. El proveedor de servicio no puede saber quién es el cliente que ha accedido, ni establecer conexiones entre los diferentes accesos de un cliente (figura 51).

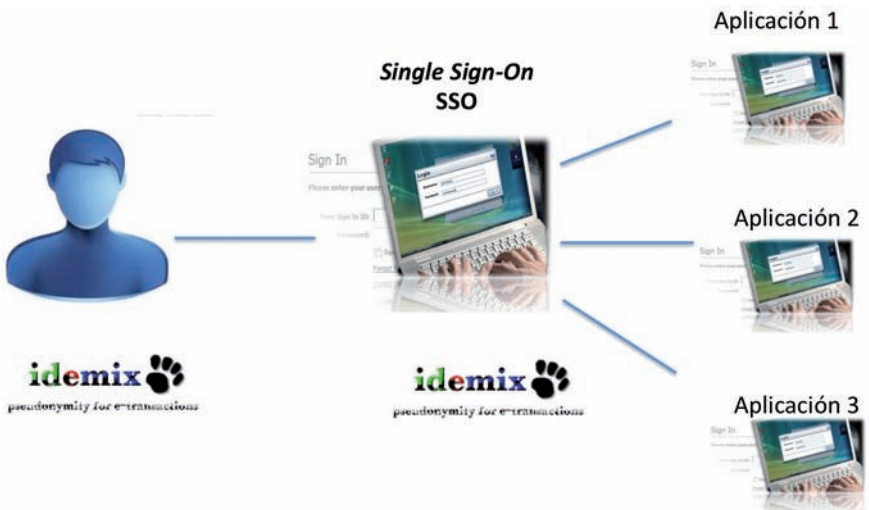
Figura 51. Proceso de suscripción con Idemix



Fuente: Jan Camenisch IBM Research, Zurich Research Laboratory.

- **Proceso de autenticación *Single Sign-On***: En muchas aplicaciones actuales y propuestas, un usuario accede a diversos servicios a través de un solo servidor que centraliza todo el acceso, tradicionalmente este servidor *Single Sign-On* (SSO) sabe qué usuario accede a qué servicio y con qué frecuencia. Esto se puede evitar simplemente con que el usuario y el servidor SSO dispongan de Idemix. Así, el usuario tendrá credenciales de todos los servicios en los que esté registrado; no obstante, cuando quiera acceder a un determinado servicio, deberá mostrar las credenciales al servidor, sin que este sea capaz de identificar qué usuario es, ni si un usuario ha realizado diferentes accesos (figura 52).

Figura 52. Proceso *Single Sign-On* con Idemix



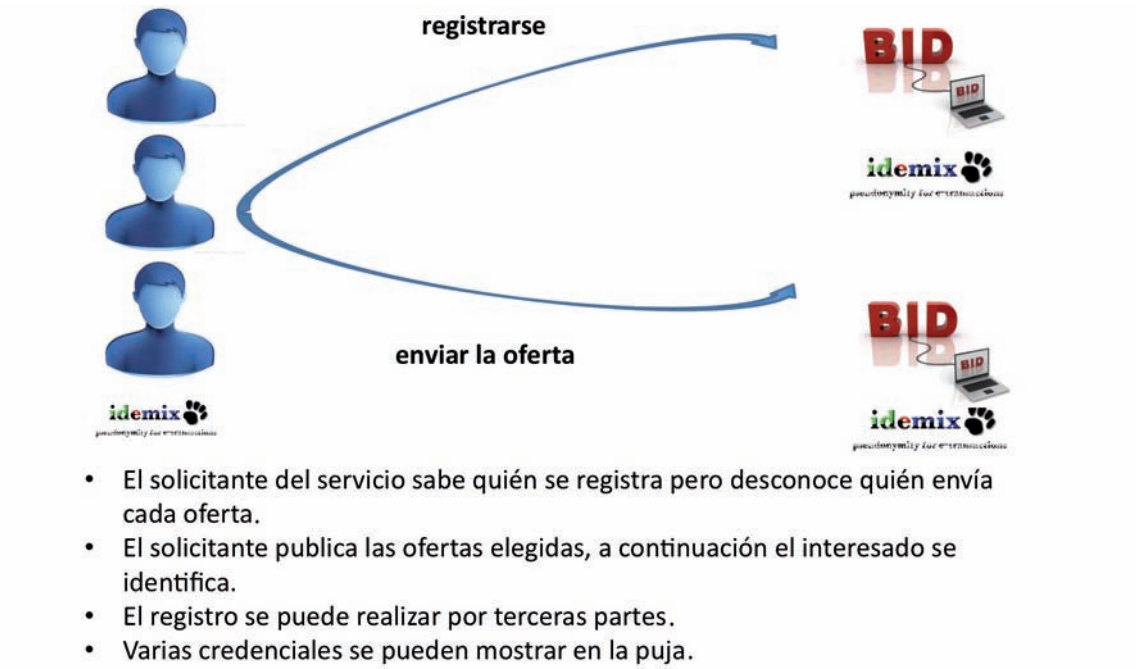
El servidor Single Sign-On (SSO) desconoce quién accede a los servicios:

- El cliente revela los atributos necesarios para una petición concreta
- Los servidores de SSO no pueden vincular las diferentes peticiones del mismo cliente.
- Solo SSO y el cliente deben instalar Idemix.
- No se comparten los atributos.

Fuente: Jan Camenisch IBM Research, Zurich Research Laboratory.

- **Proceso de pujas**: En este caso, tenemos principalmente la entidad que presenta la petición y las que contestan con sus ofertas. Cada ofertante presenta su oferta utilizando un canal anónimo y utilizando su credencial, de manera que la entidad que recibe la oferta sabe que una persona acreditada ha realizado la puja aunque no es capaz de conocer su identidad. Cuando el solicitante muestra la oferta ganadora, la entidad que ha enviado dicha oferta puede identificarse como la opción ganadora (figura 53).

Figura 53. Proceso de pujas con Idemix



- El solicitante del servicio sabe quién se registra pero desconoce quién envía cada oferta.
- El solicitante publica las ofertas elegidas, a continuación el interesado se identifica.
- El registro se puede realizar por terceras partes.
- Varias credenciales se pueden mostrar en la puja.

Fuente: Jan Camenisch IBM Research, Zurich Research Laboratory.

A.1.4 Complementos en navegadores para mayor privacidad

Los *widgets* incrustados en las webs, que permiten a los usuarios enlazar contenido en sus perfiles, permiten también a las redes sociales conocer qué webs visitan sus usuarios, incluso sin que el internauta pulse en el *widget*. Disconnect[40] es una herramienta para el navegador que permite bloquear *widgets* de terceras partes como Digg, Facebook, Google, Twitter y Yahoo. Otro ejemplo de estas herramientas es *ghosting* para Firefox.

Otra herramienta en esta línea es la de la empresa Abine, que se encarga de mejorar la privacidad *online*. Lanzada en junio de 2010, provee a los internautas de una serie de herramientas sencillas con las que controlar y proteger su información personal *online*. Entre sus servicios se encuentran TACO (Targeted Advertising Cookie Opt-out), con el que se puede desactivar la publicidad dirigida en webs como Google, Microsoft o Yahoo entre más de cien sitios, o Deleteme, con el que se puede eliminar cierta información acerca de la identidad en webs de datos como Intelious o mylife (figura 54).

40. www.disconnect.me

Figura 54. Abine

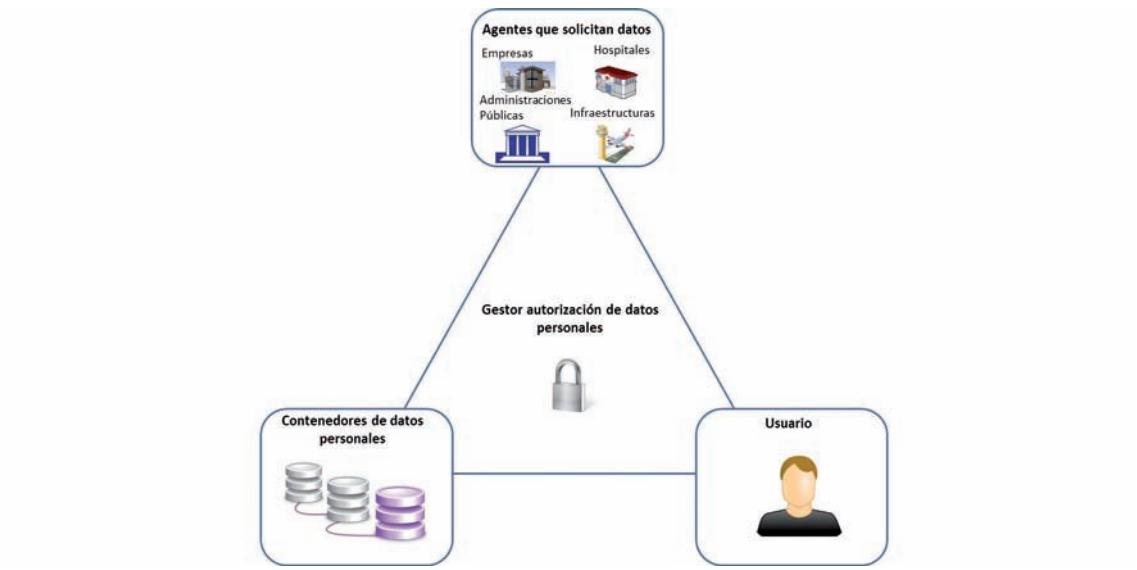
A.2 Herramientas para que el usuario simplifique la gestión de su identidad digital

En este conjunto se agrupan las herramientas que permiten la gestión de la identidad digital y que ofrecen soporte para manejar los datos personales que están en poder de terceros. Se trata de facilitar el mantenimiento correctivo de la información, la búsqueda, así como el borrado de información en el caso de que sea necesario.

El primer concepto que hay que manejar a la hora de entender las herramientas de gestión de la identidad es el número de agentes que participan generalmente en una herramienta así, y qué papel tiene cada uno. Dentro de un sistema para gestionar la identidad participan cuatro agentes, tal y como se ha descrito en un capítulo anterior:

- Los contenedores de datos personales: Se trata de aquellos agentes que, teniendo datos personales parciales de la persona, ayudan a configurar la identidad digital. Entre estos agentes se encuentran los proveedores de tarjetas de crédito, que actúan como emisores de identidad que habilitan los pagos, y los gobiernos, que emiten certificados de identidad para los ciudadanos (por ejemplo, el DNI).
- Los agentes que solicitan los datos personales: Son sitios que requieren de una identificación y que solicitan los datos que están almacenados en los contenedores de datos personales.
- El gestor de la autorización de uso de datos personales: Son los agentes que actúan de intermediarios entre los contenedores de datos personales y los agentes que los solicitan.
- Usuario: Es quien controla la interacción y el que decide qué datos se almacenan, se comparten, se publican, etc. (figura 55).

Figura 55. Componentes de un gestor de identidad digital



Fuente: Elaboración propia.

A.2.1 OpenID

OpenID es un sistema simple de código abierto para acceder a diferentes servicios en Internet sin necesidad de tener que crear una nueva cuenta, con nuevo usuario y contraseña. Se trata de un sistema de gestión de identidad descentralizado puesto que cada usuario puede tener un proveedor de identidad diferente y se centra en ofrecer SSO (*Single Sign-On*) y funcionalidades como la propagación de atributos a los diferentes servicios que lo usan. Se ha utilizado sobre todo en el mundo del software libre.

El funcionamiento de OpenID consiste en que el proveedor de identidad le otorga un identificador al usuario, identificador que puede ser bien una URL o un XRI. En el caso de que sea una URL, el proveedor de identidades registra nuestra URL como identificador de identidad. Por ejemplo, con la cuenta de Google abierta se copia la dirección URL y ya se puede usar como identificador de OpenID. En el caso de los XRI, la estructura consta de dos formas, los i-nombres y los i-números, que habitualmente se registran de forma simultánea como equivalentes. Los i-nombres son reasignables (como los nombres de dominio), mientras que los i-números nunca son reasignados. Cuando un i-nombre XRI es usado como identificador OpenID, este es resuelto inmediatamente por el i-número equivalente. Este i-número es el identificador OpenID almacenado por la parte confidente. De esta manera el usuario y la parte confidente están protegidos contra los cambios de identidad que podrían suceder con una URL basada en un nombre DNS reasignable.

A modo de ejemplo, en las figuras 56 y 57 se presentan algunos proveedores y servicios que aceptan OpenID.

Figura 56. Proveedores de OpenID

AOL	ClickPass	Yahoo!	LiveJournal	MySpace	WordPress
Blogger	Google Profile	Google	Verisign	Typepad	MyOpenID
ClaimID	Clavid	Steam	Orange	TonidoOpen ID	Launchpad
Ubuntu	Seznam.cz	Xlogon	Hyves	Mixi	Virgilio.it

Figura 57. Agentes de confianza de Open ID

Yahoo!	Flickr	Tripit
Amazon	Wikitravel	SourceForge
Facebook	Bitbucket	Thexyz

A.2.2 InfoCards

Las tarjetas de identificación consisten en un modelo federado abierto de gestión de identidad con el que se pueden elegir los tipos de información accesibles para cada servicio. Bajo este modelo, cada usuario tiene un número de identidades gestionadas a través de una aplicación (que reside en el PC del usuario y que se denomina selector de identidades). Se trata así de un sistema de autenticación y de una herramienta que permite mostrar las diferentes capas en la identidad de una persona ya que con ella es posible seleccionar la información que se da a según qué agente (datos bancarios en el caso de tarjetas de crédito, información sobre compras, etc.).

En la práctica, usar las tarjetas de identidad permite a los usuarios la autenticación sin necesidad de un nombre de usuario y contraseña para cada web (siempre y cuando las webs acepten este sistema).

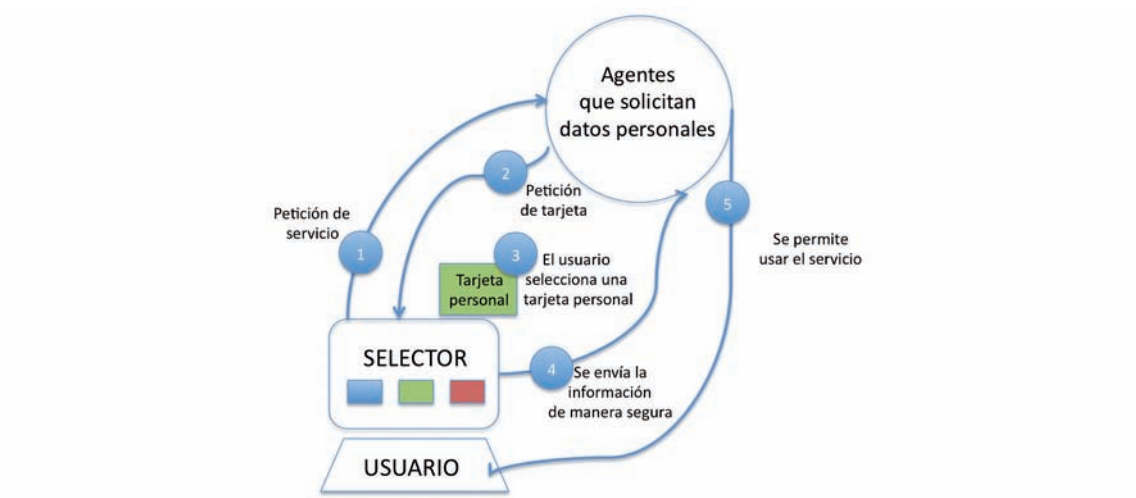
Este tipo de sistemas estaban ya definidos desde 2006 por la Microsoft Windows CardSpace y en años sucesivos se han ido complementando, lo que llevó, por ejemplo, a que en 2008 se creara la Fundación de Tarjetas de Información (Information Card Foundation) con líderes en la industria como Google, Microsoft, Oracle Corporation, Paypal, Equifax, Verizon y Deutsche Telekom.

De manera genérica, se han establecido dos tipos de tarjetas de identidad:

- Las tarjetas personales: Son un tipo de tarjetas informales, similares a una tarjeta personal física para la presentación de un profesional. Se pueden crear desde un selector de identidad y proporcionar campos como nombre, apellidos, dirección, teléfono móvil, etc. Estas tarjetas son creadas por el propio usuario, por lo que no tienen por qué ser aceptadas por todos los grupos de confianza y son almacenadas en el propio selector de identidad del usuario. Se pueden usar en webs como foros, para evitar tener infinidad de parejas de usuarios/contraseñas (figura 58).
- Las tarjetas administradas: Este tipo de tarjetas son las que ofrecen los proveedores de identidad. Son las tarjetas que provee, por ejemplo, un banco o una tienda acreditando que se es cliente, o un gobierno, en este caso a través de la identificación ciudadana. A diferencia de las identidades *offline*, la información sobre la identidad no es almacenada en local, sino que el selector de identidad utiliza un fichero XML que se descarga cuando se solicita al proveedor de identidad. Ese fichero permanece guardado en el PC del usuario o en su defecto en un servicio de *cloud computing*, pero no contiene la información. Cuando se quiere acceder a un servicio y los agentes que solicitan datos de identidad digital piden una identificación, el selector de identidad da a elegir entre todas las identidades disponibles. Una vez seleccionada una identidad, se envía una petición desde el usuario/selector de identidad hacia el proveedor y este le devuelve la información de una manera segura. Esa información podrá ser verificada por el usuario (en caso de ser necesario) y este envía la información a su vez al agente que solicitó la información, el cual comprueba los datos y da acceso al servicio (figura 59).

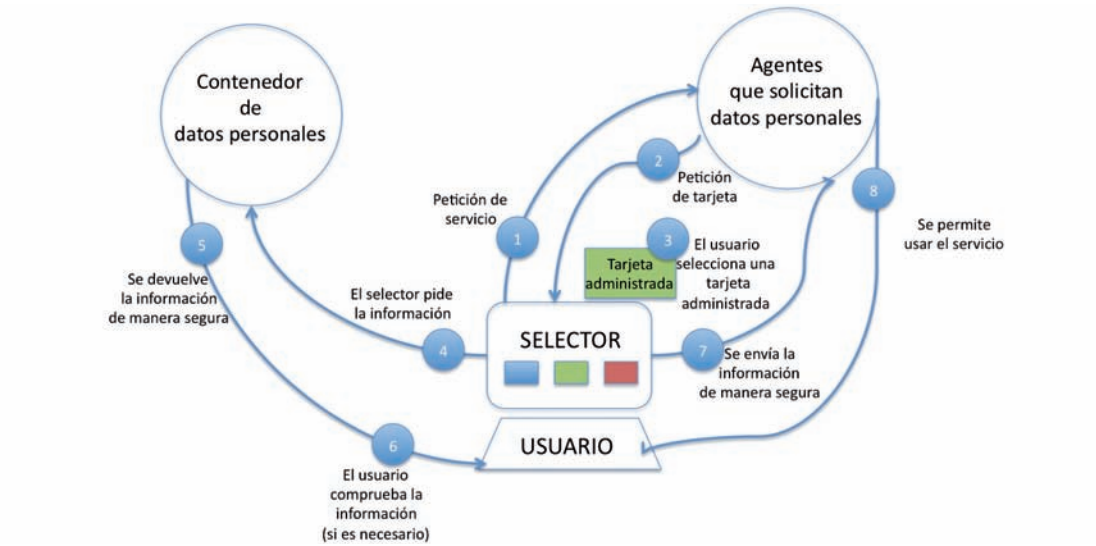
Se puede decir así que al igual que las carteras permiten organizar las identidades en el mundo físico a través de diferentes tarjetas, los selectores de identidad permiten gestionar la identidad digital.

Figura 58. Funcionamiento de las tarjetas personales



Fuente: Elaboración propia.

Figura 59. Funcionamiento de las tarjetas administradas



Fuente: Elaboración propia.

Por otro lado, en el marco de otros proyectos, como en el de *open source* Higgins, se están desarrollando nuevos tipos de tarjetas.[41] Es el caso de las tarjetas de relación (R-Cards), que son tarjetas personales que contienen campos donde se guarda la información. Las tarjetas administradas contienen la dirección del proveedor de identidad que contiene los datos organizados por campos, al igual que en las tarjetas personales. Los agentes que solicitan los datos personales acudirán a estos proveedores de identidad a solicitar la información. La novedad con este tipo de tarjetas es que se deja abierta una comunicación entre el proveedor de identidad y el agente que solicita datos de manera que este también pueda escribir datos en los campos que almacenan la información sobre la identidad digital (en el caso de que se tengan permisos para ello). Al igual que las tarjetas personales y administradas, en las tarjetas de relación también existirán tarjetas de relación personales en las que la comunicación se mantiene entre el usuario y el agente que solicita información, y las tarjetas de relación administradas en las que la relación se establece entre el proveedor de identidad o contenedor de los datos y el agente que solicita información.

Otros ejemplos de selectores de identidad son la CardSpace de Windows, DigitalMe y las diferentes versiones de Eclipse Higgins Project.

El uso de tarjetas de información es muy útil y genera oportunidades de negocio tanto a los agentes que proveen la identidad como a los que solicitan los datos personales.[42] En el caso de los agentes que solicitan los datos, se facilita notablemente el proceso de rellenado de formularios de registro. Además, los usuarios de tarjetas de identificación pueden ser clientes muy espontáneos e impulsivos. Por ejemplo, un usuario de tarjetas de identificación puede terminar el proceso de compra en un solo clic por lo que atraer a este tipo de clientes es una oportunidad.

41. http://eclipse.org/higgins/
42. http://informationcard.net/business-information-center

En el caso de los proveedores de identidad, es decir, de los agentes contenedores de datos personales, el uso de las tarjetas de información permitiría desbloquear información crítica, no solo acerca de sus usuarios, sino de cómo ciertos usuarios interactúan en la comunidad. Reputación, relaciones o pagos son algunas de las ventajas que puede ofrecer el contenedor de datos a sus *partners* o afiliados, con la aprobación activa del usuario, como parte de una transacción en tiempo real. El convertirse en proveedor de identidad digital será considerado por los usuarios como un valor añadido y además esa comunidad se convertirá en una parte de su vida. Es decir, si un usuario elige a un agente como representante de su identidad, estará invirtiendo en su relación con ese agente mucho más que si únicamente perteneciera a la comunidad. De hecho, siendo proveedor de identidad, el compromiso con los usuarios es muy alto. Así, el uso de las tarjetas de información significa proveer de seguridad y privacidad lo que permitirá que la relación con los usuarios sea más fuerte que nunca.

En resumen: desde el paradigma de las tarjetas de identidad se puede hacer ver al usuario que los datos pasan de consumirse en sitios sin ningún tipo de control a tener un sistema avanzado de comunicación segura que mejora la confidencia con el fin de protegerlos. La combinación entre nuevas vías de compartición de datos y la mejora sustancial en las relaciones con los clientes da una potente plataforma para imaginar nuevos servicios.

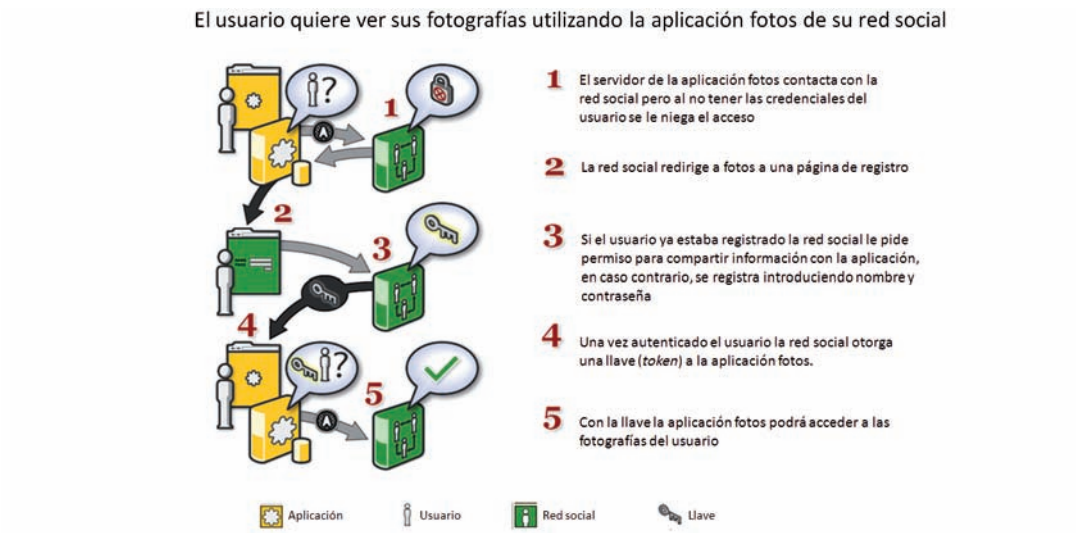
A.2.3 OpenSocial y OAuth

OpenSocial es una tecnología empleada para gestionar el acceso a la información de los usuarios a través de la web. Se utiliza para acceder a datos sobre personas, sus contactos e información personal contenidos en una red social o similar. Gracias a ella otras aplicaciones ajenas a la red social o servicio utilizan esta tecnología como una llave para acceder a los datos personales almacenados en ella. OpenSocial se apoya en el protocolo de autenticación OAuth[43] y delega así el control de la privacidad en la red social contenedora de la información.

OAuth permite la autorización segura y sencilla de aplicaciones de escritorio y aplicaciones web. Esta tecnología se supone novedosa por no comprometer las credenciales durante la comunicación entre un sitio contenedor de información personal y otro solicitante de esta información. Típicamente, el contenedor de información es una red social y el solicitante un servicio tercero, como podría ser un juego o una aplicación de fotos. Por tanto, continuando con este ejemplo, si un usuario está «logueado» en su red social, donde almacena fotografías, cuando accede a la aplicación de fotos, tradicionalmente, esta debería volver a aportar las credenciales del usuario y así tener acceso a su información, sin embargo, con esta tecnología es OAuth quien se encarga de verificar la identidad y autorización del usuario haciendo innecesario volver a loguearse, de manera que se reduce la vulnerabilidad de las credenciales (figura 60).

43. Open Authorization.

Figura 60. Caso de uso de OpenSocial y OAuth



Fuente: opensocial.org

OAuth introduce un tercer rol a la tradicional autenticación de cliente-servidor: el propietario de la información. En el modelo OAuth, el cliente (que no tiene por qué ser el propietario de la información, sino que actúa en su nombre) hace la petición de acceso a los datos controlados por el propietario de la información en el servidor.

Por ejemplo, un usuario (propietario de la información) puede garantizar a un servicio de imprenta (cliente) el acceso a su lugar de almacenamiento de imágenes (servidor) sin cederle su usuario y contraseña al servicio de imprenta. El propietario de la información se autenticaría contra el servidor directamente y al servicio de imprenta se le delegarían ciertas identidades.

Otro ejemplo de aplicación de estas tecnologías (tanto OpenSocial como OAuth) es MySpaceID que permite a los usuarios de MySpace compartir su información social, almacenada en la red social, con aplicaciones externas, es decir, gestiona el acceso a la información y el proceso de autenticación.

Por su parte, la API Graph es el núcleo de la plataforma de Facebook, que permite leer y escribir en una cuenta de dicha red social. La plataforma de Facebook usa el protocolo de autenticación OAuth 2.0 para la autenticación y autorización, mientras que para el acceso a la información utiliza tecnología propia en vez de OpenSocial, decisión que se ha ganado un fuerte rechazo por parte de la comunidad.

A.2.4 W3C[44] *social web incubator group*

El objetivo de este grupo es entender los sistemas y las tecnologías que permiten la descripción e identificación de personas, grupos, organizaciones y contenidos generados por los usuarios respe-

44. World Wide Web Consortium.

tando los aspectos de privacidad. En este sentido, el grupo no lanza iniciativas concretas, sino que se limita a ser un mero recolector de distintas ideas relacionadas con la identidad digital. Su objetivo final es crear un informe que permita ofrecer una visión global de las iniciativas existentes, y que ayude en el trabajo de estandarización que se realiza en el W3C. Como arquitectura de la red social, proponen un conjunto de macros de aplicación o *frameworks* que interoperen a partir de formatos y protocolos comunes estandarizados.

A.2.5 Kantara

Kantara nace como una iniciativa promotora de la reunión y concreción de las distintas soluciones para la gestión de la identidad. Es decir, pretende aunar los esfuerzos de diferentes iniciativas como Liberty, Concordia, DataPortability o Information Card Foundation para lograr estandarizar las múltiples soluciones relativas a la identidad existentes hoy en día y poder continuar su evolución en una misma dirección.

A.2.6 Federación de identidades y SAML

La identidad federada es una de las soluciones para abordar la gestión de identidad en los sistemas de información. El valor añadido adicional respecto a otras soluciones es la gestión de identidad interdependiente entre compañías. El objetivo es obtener una gestión de usuarios eficiente, la sincronización de los datos identificativos, la gestión del acceso, los servicios de directorio, la auditoría e informes...

Mediante soluciones de Identidad Federada los individuos pueden emplear la misma identificación personal (típicamente usuario y contraseña) para identificarse en redes de diferentes empresas o servicios de Internet. De este modo, las empresas comparten información sin compartir tecnologías de directorio, seguridad y autenticación, como requieren otras soluciones. Para su funcionamiento es necesaria la utilización de estándares que definan mecanismos que permiten a las empresas compartir información entre dominios. El modelo es aplicable a un grupo de empresas o a una gran empresa con numerosas delegaciones y se basa en el «círculo de confianza» de estas, un concepto que identifica que un determinado usuario es conocido en una comunidad determinada y tiene acceso a servicios específicos.

El término SAML (Security Assertion Markup Language), por su parte, se refiere a la sintaxis y la semántica usados para el transporte de *tokens* seguros entre los proveedores de identidad y los grupos de confianza o agentes que solicitan los datos.

A.2.7 Herramientas que habilitan los pagos privados

Los intermediarios de transacciones son modelos de negocio muy conocidos. En el contexto tradicional Visa y MasterCard son las más populares. Estas empresas intervienen como intermediarios entre los comerciantes y los titulares de las tarjetas de crédito.

En el ámbito de Internet se precisan también estos intermediarios por una simple razón de confianza. En este sentido, PayPal es una de las empresas mejor posicionadas cuya labor es la de conferir dicha seguridad dotando de confianza a todo el proceso, tanto para el que vende, como para el que compra.

Para usar esta herramienta el procedimiento es el siguiente: con una cuenta de correo electrónico es posible crearse una cuenta PayPal. En ella, cada usuario tiene un balance de dinero virtual que puede recargar a través de una tarjeta de crédito o realizar la compra directamente y cargar el importe a la tarjeta pero con Paypal como intermediario. Por lo tanto, al final el proceso de compra finaliza simplemente introduciendo los datos de correo y la contraseña de la cuenta Paypal y más tarde Paypal carga el importe a la cuenta bancaria que esté asociada o tarjeta de crédito[45].

A.2.8 Navegadores que soportan diferentes perfiles

Otro ejemplo de herramientas que facilitan la gestión de la identidad digital son las que permiten a los navegadores soportar diferentes perfiles. Es frecuente que las identidades de un usuario en Internet varíen o que incluso un mismo dispositivo pueda ser usado por diferentes personas a las que no les interesa que se conozca el historial del otro o las contraseñas guardadas, por ello es razonable que aparezcan este tipo de herramientas de navegación con las que poder seleccionar la identidad con la que acceder a Internet.

Un ejemplo concreto de ello sería el de la aplicación para iPad, Passtouch, con la que acceder con diferentes identidades que se seleccionan mediante la ejecución de patrones al iniciar la aplicación (figura 61).

Figura 61. Acceso mediante un patrón a Passtouch

Fuente: www.passtouch.com

45. https://www.paypal.com/es/cgi-bin/webscr?cmd=xpt/Marketing/general/NewConsumerWorks-outside

A.2.9 Herramientas de análisis de los perfiles de navegación en portales

Los usuarios se relacionan con las empresas de forma digital a través de sus portales. Durante la navegación por dichos portales, los usuarios muestran diferentes pautas de comportamiento que pueden ser analizadas por las empresas, así estas crean perfiles de los usuarios que les permiten dirigir los esfuerzos comerciales de forma más adecuada e incluso personalizar las ofertas.

Son varias las empresas que han visto en esta situación un hueco de mercado y en la actualidad han desarrollado aplicaciones para crear perfiles de clientes a terceras empresas, por ejemplo Celebrus y Baynote, como se muestra en la figura 62. Se trata de plataformas que se alimentan de datos de la navegación de los usuarios en los portales de empresas de venta *online* y que llevan incorporados módulos para el análisis de la información proveniente de esta navegación, lo que permite mejorar la interacción con los usuarios. De una forma simplificada, se puede considerar que todas estas herramientas tienen tres módulos:

- Captura de datos: Se encarga de recoger los datos de navegación de los usuarios, ya sea desde terminales fijos o desde terminales móviles y, generalmente, en tiempo real.
- Transformación: Los datos sobre actividad de los usuarios se transforman en modelos de comportamiento de datos y, en general, en información que puede ser interesante desde el punto de vista de negocio.
- Entrega de información: En el caso de que esta transformación se produzca en tiempo real, la empresa tendrá posibilidades de actuar de forma instantánea sobre el cliente, tratando de mejorar los ratios de venta. También se pueden obtener informes que permitan orientar la estrategia *online* de la compañía y las políticas comerciales.

Figura 62. Herramientas para el *profiling* de usuarios según la navegación en portales