(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 558 169**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.08.2012 E 12761562 (3)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2015 EP 2751973**

(54) Título: **Método para controlar el acceso de datos personales de un usuario**

(30) Prioridad:

02.09.2011 US 201161530416 P
29.11.2011 EP 11191213

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.02.2016

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

NICOLAS, CHRISTOPHE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para controlar el acceso de datos personales de un usuario.

Introducción

[0001] Con el desarrollo de redes de comunicación, se solicita cada vez más a los usuarios de estas redes que cedan datos personales a los proveedores de servicio para introducir tales datos personales en bases de datos.

[0002] A medida que el entorno informatizado aumenta en importancia y rendimiento, el usuario medio está cada vez más frustrado por motores informáticos de mala calidad que se preocupan muy poco acerca de sus necesidades de privacidad.

Estado de la técnica

[0003] Algunos terceros ponen un valor alto en los datos personales que un individuo introduce en varios sistemas conectados que forman parte de su vida cotidiana.
El uso que tales terceros pueden hacer va desde estudios de mercado para la publicidad dirigida hasta minería de datos y similares.

[0004] Hasta el momento, no ha habido marco o estructura para:
1) permitir al usuario tener un control completo de su datos personales;
2) convencer al usuario de que no corre un riesgo desproporcionado dando tales datos;
3) como otro paso posible, monetizar formalmente los datos personales enviados, gracias a la confianza del usuario, como beneficio directo para dicho usuario.

[0005] La calidad de las bases de datos puede verse afectada negativamente por la desconfianza de los individuos.
En el caso de un censo, por ejemplo, algunos usuarios de libre pensamiento adoptan comportamientos anti-sistema al proporcionar datos falsos, sólo porque no confían en la entidad gubernamental que está solicitándoles que proporcionen estos datos.

[0006] Cuando los datos proporcionados están claramente fuera de rango, la limpieza del flujo de resultados es relativamente fácil y puede hacerse de forma automatizada, por ejemplo a través de controles cruzados simples entre respuestas proporcionadas por un único usuario.
No obstante, cuando el librepensador es más sofisticado y sabe cómo ser más listo que las verificaciones automatizadas, hay muy poco que pueda hacerse para obtener datos reales y una calidad buena resultante de bases de datos agregadas.

[0007] Se necesita por lo tanto un sistema que esté diseñado para dar control completo y continuo de sus datos por un usuario, ganar la confianza del individuo medio, alentando a tal individuo a convertirse en un usuario abierto de mente y que confíe en dicho sistema.

[0008] El problema se ha agudizado con la creciente popularidad, especialmente entre jóvenes adultos, de las redes sociales.
Los gestores de varias redes sociales de este tipo tienden a tener poca consideración hacia cualquier desventaja futura por la falta de experiencia de estos jóvenes adultos frente a los problemas de percepción que un visitante de tales redes sociales puede encontrar.

[0009] Por ejemplo, un joven descuidado puede publicar en su memoria personal, acogida por una red social, algún material visual al que él, pensándolo mejor o años después, preferiría restringir el acceso. Tales materiales visuales pueden ser por ejemplo vídeos o fotografías hechos durante una fiesta privada, durante la que el alcohol, o más generalmente sustancias capaces de modificar el estado de conciencia, fueron ingeridas o inhaladas.

[0010] Cuando dicho joven descuidado se convierte en un graduado en busca de trabajo, el hecho de que una red social dio acceso, mediante unas audiencias no restringidas o no restringidas lo suficiente, a indicios de dicho modo de vida ilustrado por las imágenes mencionadas anteriormente puede ser una desventaja para encontrar un trabajo deseado.

[0011] Si dicho joven emprende una carrera política, las repercusiones pueden ser incluso más graves, con pruebas de una vida pasada como un hombre o una mujer joven o mujer siendo mostradas por la prensa a un gran público, especialmente un público mayor o de edad avanzada con poca inclinación a perdonar, lo que minaría así la credibilidad de la persona en cuestión, aunque esa persona pueda haber madurado y pueda lamentar su comportamiento pasado de joven.
El continuo almacenamiento, en bases de datos fuera del alcance, de extractos de publicaciones hechas por jóvenes puede así volverse muy perjudicial para su futuro profesional o político.

[0012] El problema se hace más serio por el hecho de que los gestores de las redes sociales a veces tienden a sobreproteger su organización, en caso de enterarse de problemas relacionados con la propiedad de datos, alterando los términos legales aplicados a los miembros individuales de una red social dada.

[0013] En tal caso, una falta de consideración por los intereses de dichos miembros individuales puede resultar en el daño grave a dichos intereses.
Por ejemplo, las condiciones legales son a veces modificadas sin previo aviso, reivindicando la propiedad por parte de la red de cualquier dato y de todos los datos enviados en el almacenamiento personal del individuo.

[0014] Aunque la información sobre tal cambio en términos legales se comunique a los suscriptores, hay una probabilidad alta que una gran mayoría de los usuarios más jovenes no reaccione y por lo tanto acepte implícitamente tal cambio.
E incluso si algunos reaccionan y solicitan una eliminación de los datos incriminados, se enfrentan a la perspectiva de una acción legal costosa contra dicha red social, con éxito incierto.
El coste de tal acción legal para un individuo, en comparación con los recursos frecuentemente desproporcionados disponibles para la red social como parte demandada, puede disuadir al individuo de iniciar tal acción en absoluto, lo que conlleva un sentimiento de frustración por su parte.
El número de casos en los que la credibilidad, o la vida personal, o el futuro profesional un individuo es minado/a, o deteriorado/a, o comprometido/a está en aumento, y también lo está la cobertura por parte de la prensa de tales historias, al igual que el resultante interés del público.

[0015] Con el aumento de este número de casos, una consecuencia de los hechos mencionados anteriormente es una actitud defensiva aumentada del público general ante las redes sociales.
No obstante, las redes sociales están de moda y ganan más popularidad entre el público más joven.
Esto las hace inevitables en gran parte para las personalidades ambiciosas, que no siempre se dan cuenta del peligro que representan para su vida social futura.

[0016] El documento US 2010/0088364 describe contenido de las redes sociales que se puede presentar a un conjunto de usuarios de redes sociales.
El contenido de redes sociales presentado puede incluir contenido semántico asociado a usuarios específicos de redes sociales.
El contenido semántico puede ser compartido entre diferentes usuarios de los usuarios de redes sociales durante la presentación.
Al menos una parte del contenido semántico se puede almacenar dentro de una memoria de datos local asociada a un dispositivo informático del usuario específico al que se aplica el contenido semántico.

Breve descripción de la invención

[0017] Se propone un método para controlar el acceso a datos personales de un usuario por un centro de confianza que comprende al menos una base de datos que comprende, para un usuario específico, ubicaciones de memoria para datos personales, condiciones de acceso asociadas a los datos personales y datos de gestión que comprenden al menos un contador,

- carga por parte de un usuario en la base de datos del centro de confianza sus datos personales y asignación de condiciones de acceso a dichos datos, dichos datos personales siendo divididos en al menos dos categorías con dos condiciones de acceso diferentes, cada categoría siendo asociada a un valor del usuario,

- solicitud de acceso al centro de confianza por una tercera parte a los datos personales de una pluralidad de usuarios, donde dicha solicitud comprende criterios de búsqueda,

- ejecución por parte del centro de confianza de los criterios de búsqueda en los datos personales de los usuarios para determinar un primer conjunto de usuarios que coinciden con los criterios de búsqueda,

- devolución a la tercera parte de información que muestra la cantidad del primer conjunto de usuarios que coinciden con el criterio, al igual que la suma del valor de usuario de cada usuario del primer conjunto,

- reconocimiento de toda o parte de la suma por la tercera parte, definiendo así un segundo conjunto de usuarios que puede comprender todo o parte del primer conjunto,

- devolución de los datos personales del segundo conjunto de usuarios para el que la suma cubre los valores acumulados de los usuarios extraídos,

- actualización del contador del segundo conjunto de usuarios con el contenido del valor de sus datos personales respectivos.

Breve descripción del dibujo

[0018] La presente invención será entendida mejor gracias a las figuras adjuntas, donde:

- la figura 1 muestra un sistema con el centro de confianza conectado a Internet

- la figura 2 muestra un sistema donde el centro de confianza tiene la función de un proxy.

Descripción detallada

[0019] La invención consiste en un sistema de suscripción a un centro de confianza TC abierto por lo menos a una parte del público general, donde se alienta a un miembro suscriptor, a través de rasgos de sistema definidos, a tener un control completo de sus datos personales una vez éstos se han introducido en el sistema.
El miembro suscriptor es por lo tanto alentado a proporcionar datos reales al centro de confianza.

[0020] Tales rasgos del centro de confianza definido TC pueden consistir en estándares mínimos de calidad en el tratamiento de dichos datos proporcionados.
Por ejemplo, algunos sistemas existentes son capaces de llegar a descubrir el hecho de que un usuario de internet ha visitado sitios web de hoteles en Italia, e inmediatamente proponer ofertas de viajes a Italia con descuento a ese usuario.
Tales ofertas se pueden percibir como publicidad intrusiva e indeseada.
Un estándar mínimo de calidad puede consistir en la definición, con cada usuario individual, de hasta qué punto tales ofertas automatizadas se pueden generar y mostrar.

[0021] Otra característica de sistema definida puede también consistir en proporcionar la posibilidad de eliminar verdaderamente y de forma fiable un historial de datos para el usuario individual.

[0022] En una forma de realización particular de la invención, una característica del sistema está diseñada para proporcionar transparencia completa a un usuario suscriptor.

[0023] En una forma de realización particular de la invención, el sistema proporciona un nivel diferenciado de control a un usuario suscriptor, sobre el tipo de datos que él introduce en el sistema.

[0024] Como primer ejemplo, una primera categoría de nivel de control se asigna a las preferencias del usuario en deportes.
Tales datos de preferencia pueden consistir en sus valoraciones personales en deportes.
Por ejemplo, un usuario A deja al sistema saber que él prefiere el baloncesto al fútbol, el fútbol al tenis, y el tenis al windsurfing.
Tales datos de preferencia también pueden consistir en valoraciones personales sobre varios equipos participantes en un deporte dado.
Como otro ejemplo, un usuario B puede revelar, con un nivel determinado de propiedad y control, la información de que él prefiere un determinado equipo de baloncesto a otro equipo de baloncesto dado.

[0025] Como segundo ejemplo, se asigna una segunda categoría o nivel de control a los hobbies del usuario.

[0026] Como tercer ejemplo, un segundo nivel de control se asigna a la orientación política del usuario.
Datos sobre la orientación política pueden por lo tanto ser considerados, por el usuario, como más delicados que las preferencias sobre deportes o hobbies, y ser concedidos un nivel más restrictivo de protección contra acceso externo que no sea del usuario.

[0027] Como cuarto ejemplo, un tercer nivel de control se asigna a las preferencias orientación o hábitos sexuales del usuario.

[0028] Como ejemplo adicional, un nivel de control se asigna a las características de perfil de inversor del usuario.
Tales características pueden ser conservadurismo financiero, tolerancia al riesgo, inclinación a las inversiones alternativas, al comercio justo o preferencias de preservación de la naturaleza en las opciones de inversión, o similares.

[0029] En una forma de realización particular de la invención, el sistema proporciona un nivel diferenciado de control sobre los diferentes tipos de datos tal y como se ha mencionado anteriormente.

[0030] Este control se puede ejecer de formas diferentes:

a) directamente a través de opciones explícitas,

b) indirectamente, por ejemplo a través de la definición de reglas de acceso,

c) mediante proxy, es decir, subcontrayendo un nivel de control a un tercero de confianza.

[0031] Para cada categoría, el usuario puede definir un valor del usuario que representa el valor de esta información para dicha categoría.
Se pueden aplicar distintas maneras de completar este valor.

- el usuario puede definir libremente el valor

- el sistema propone valores predefinidos, y el usuario selecciona uno

- el valor es automáticamente añadidoo por el sistema y simplemente reconocido por el usuario.

[0032] Cabe observar que el usuario puede decidir no compartir una categoría particular de sus datos personales.

[0033] De hecho, cuando una categoría coincide con el criterio de búsqueda del tercero, no se reenvía la categoría de nuevo a la tercera parte, sino la identificación de usuario.
Para una categoría dada, por ejemplo deporte, el usuario puede también decidir qué parte de su identificación es enviada.
El usuario puede seleccionar una dirección de correo electrónico dirección, un nombre, una ubicación, una cuenta de twitter o de facebook, es decir, información que puede utilizarse para permitir que el tercero proponga servicios o productos a dicho usuario.

[0034] El método anteriormente descrito se puede usar en un nivel más abstracto y de forma anónima.
La tercera parte podría estar sólo interesada en el número de clics para un criterio de búsqueda específico.
Por ejemplo, una empresa, antes de la apertura de una tienda deportiva en una ubicación específica, puede solicitud al centro de confianza obtener el número de gente que son asiduas del deporte en una zona geográfica cercana a la futura tienda.
En este caso, el centro de confianza no reenvía la identificación del usuario.

[0035] En este caso, cada categoría de los datos personales pueden tener de hecho dos valores del usuario, uno para tener acceso a la identificación del usuario y otro para simplemente participar en esta búsqueda anónima.

[0036] El resultado de la búsqueda puede dar un gran número de clics.
Por este motivo el presente método propone algunas características de optimización.
En el caso de que el valor del usuario pueda tener contenido diferente, es decir, para un usuario, 0,1 céntimos y para otro usuario, 0,2 céntimos, el centro de confianza organizará los datos transmitidos al tercero mediante agrupamiento de los usuarios con la misma cantidad.
El centro de confianza presenta la información por cantidad, por ejemplo 1200 usuarios a 0,1 céntimos y 2300 usuarios a 0,2 céntimos (de los usuarios que satisfacien el criterio de búsqueda).
La tercera parte puede luego decidir refinar la búsqueda añadiendo criterios de búsqueda adicionales y volver a realizar la solicitud al centro de confianza o puede aceptar la cantidad propuesta para el primer conjunto de usuarios.

[0037] En el criterio de búsqueda enviado por la tercera parte, esta última puede incluir un valor límite.
Este valor definirá cuántos clics serán devueltos al tercero por el centro de confianza.
Este valor límite corresponde al valor del usuario acumulado hasta que se alcanza el valor límite.

[0038] Es bien conocido que el interés por los datos personales es más alto si éstos son precisos.
Por eso el centro de confianza puede efectuar varias verificaciones en los datos personales con o sin la ayuda del usuario.
El usuario puede tener un interés en que su datos sean convalidados, permitiendo así un valor más alto para cada categoría.
La verificación se centrará en la edad, género, dirección y otros datos personales.
Es más difícil verificar preferencias tales como color preferido, destino de vacaciones etc.

[0039] Cuando el perfil de usuario es verificado por el centro de confianza, el centro de confianza puede aumentar el valor del usuario.
La tercera parte puede también incluir en el criterio de búsqueda la posibilidad de acceder sólo a usuarios convalidados (y normalmente paga más) o a todos los usuarios.

[0040] En la figura 2, la forma de realización ilustra el caso en el que el centro de confianza TC hace la función de un proxy.
Los usuarios varios UT1, UT2 primero se conectan al centro de confianza TC y de este centro, tienen acceso a las páginas webs de la tercera parte TPWS1, TPWS2.
En este caso, el usuario primero se conecta a través del centro de confianza TC a un sitio web de la tercera parte

TPWS. Entonces, la funcionalidad del TC podría ser transparente y la identificación y autentificación del usuario tendrán lugar en una fase posterior.

[0041] En otra forma de realización, el proxy autentifica el usuario antes de acceder al TPWS.

[0042] El TPWS luego solicita la identificación del usuario y esta solicitud se pasa al TC. Este último puede controlar si los datos personales (todos o parte de ellos) del usuario son accesibles a este TPWS. En caso de que sí, los datos personales son enviados de nuevo al TPWS. Además de eso, el usuario se puede identificar por un identificador único para dicho TPWS, este identificador que es el mismo cada vez que el usuario se conecta al TPWS pero único para dicho TPWS.

[0043] En una forma de realización particular de la invención, el sistema proporciona un nivel diferenciado de control sobre los datos a través de rasgos de encriptación diferentes aplicados a los datos.
Según una primera forma de implementación de la invención, el usuario, a través de su terminal de usuario UT, se conecta a un centro de confianza TC y carga sus datos personales, gracias a una comunicación segura entre el usuario y el centro de confianza.

[0044] Como se explicado anteriormente, los datos personales se dividen en categorías y cada categoría se asigna a un derecho de acceso particular.
En el derecho de acceso, se pueden definir diferentes datos como la tercera parte que tiene acceso permitido a estos datos.
Este ajuste puede ser en forma de una lista de páginas webs de terceros (por ejemplo Facebook™, Twitter™, Linkedln™) que el usuario mete si los datos de esta categoría son accesible a este sitio web de terceros.
Los datos personales podrían también ser dibujos, textos de películas.

[0045] Además, es posible definir reglas para el aprovechamiento de los datos personales tales como la definición de la compensación financiera en el caso de que los datos personales se transfieran a un tercero.
Para cada categoría de datos personales, una cantidad particular puede ser definida.

[0046] El servicio de red de terceros TPWS puede también registrarse en la base de datos de confianza TDB. Un perfil se puede definir al igual que una descripción del tipo de actividad (por ejemplo actividades deportivas, información).
Este tercero puede definir el tipo de usuarios que le interesan, tales como hombres jóvenes o personas con animales domésticos.

[0047] Este servicio de red también puede definir la compensación para acceder a los datos personales del usuario que coinciden con las categorías de interés por este servicio de red, esta compensación podría ser asociada al registro del usuario entero o dividido por categoría de datos del usuario.

[0048] En un segundo paso, el usuario accede a un sitio web de un tercero TPWS y es invitado a identificarse.
Para la obtención de los datos personales por el sitio web del tercero, este último inicia una conexión segura con el centro de confianza y transmite la identidad del usuario así como un identificador del sitio web del tercero.

[0049] El centro de confianza entonces autentificará al usuario a través de esta conexión y solicitará la credencial del usuario.
Esta puede ser en forma de una contraseña o estar basada en una operación más segura que implica una contraseña de un solo uso (utilizando una tarjeta personal que genera esta contraseña temporal).
Una vez el usuario ha sido autentificado, el centro de confianza verifica las condiciones de acceso a los datos personales que utilizan el identificador del sitio web del tercero.
A la vista de esta verificación, los datos personales son (o no son) devueltos al sitio web del tercero.

[0050] La solicitud al centro de confianza puede también incluir información de filtro.
El sitio web de la tercera parte puede estar interesado sólo en una parte de los datos personales (al usar el descriptor de los datos) o también puede limitar el tipo del tamaño de los datos.
En caso de que los datos personales comprendan una película de 500 Mbytes, el sitio web de la tercera parte puede especificar el tamaño máximo de los datos solicitados.
En cambio o además del tamaño, el sitio web de la tercera parte puede especificar el tipo de datos en el que está interesado, por ejemplo preferencias, imágenes, etc.

[0051] Para identificar al usuario, la tercera parte puede recibir un identificador único del centro de confianza, identificador que identifica el usuario por un lado pero que es único para la tercera parte por otro lado.
En este caso, la tercera parte recibe los datos personales del usuario actualmente accediendo a sus servicios sin conocer la identidad real del usuario.
Durante el proceso de autentificación, la tercera parte puede también añadir alguna/s categoría(s) de interés y transmitirlas al centro de confianza.
Este último puede luego verificar si el usuario actualmente autentificado corresponde con la categoría identificada

por la tercera parte y, en caso de que sí, los datos personales del usuario se pueden transmitir a la tercera parte.
En el caso de que el usuario haya definido una compensación financiera, y de que ésta haya sido aceptada por la tercera parte, se hace un crédito en la cuenta del usuario, crédito proporcionado por la tercera parte.
El contador del usuario se incrementará entonces.

[0052] Como se ha explicado anteriormente, el centro de confianza puede hacer la función de proxy.
La base de datos del centro de confianza contiene los datos personales y el proxy identifica primero al usuario.
Una vez identificado, el centro de confianza puede vigilar la comunicación entre el terminal de usuario y un sitio web.
Cuando el usuario ha bloqueado algunos datos personales, tales como el número telefónico, el centro de confianza puede advertir al usuario en el caso de que el número telefónico sea solicitado.
Para el modo de proxy, el objetivo es de atrapar datos personales que transiten del usuario al sitio web.
Es difícil bloquear un sitio que solicite datos personales pero es fácil bloquear los datos que nosotros conocemos (es decir, los datos dados por el usuario al centro de confianza).
En este modo, el proxy actúa como un dispositivo DLP (de prevención de pérdida de datos).

[0053] En una versión más ligera, es posible cargar una aplicación de software pequeña en el ordenador del usuario para almacenar su identificación de usuario para el centro de confianza.
Cuando el usuario accede a un servicio de redde un tercero, teniendo él mismo una cuenta con el centro de confianza, el usuario puede autorizar el acceso a sus datos personales a este tercero (generalmente a cambio de una compensación).
Esta autorización puede ser en forma de clic en un logo del centro de confianza en la página web de la tercera parte.
Para mantener el anonimato del usuario, la tercera parte transmite a la aplicación del usuario un identificador (IDTP) del tercero.
La aplicación del usuario almacena el identificador del usuario (IDU), una clave personal (KUpr), la clave privada de un par de claves asimétricas, y una clave del centro de confianza (KTpu), la clave pública del centro de confianza.

[0054] La aplicación del usuario genera dos criptogramas, el primer criptograma $(IDU)_{KTpu}$ es obtenido por la encriptación del identificador del usuario IDU con la clave de centro de confianza KTpu, y el segundo criptograma $(IDTP)_{KUpr}$ se obtiene por la encriptación del identificador del tercero IDTP por la clave personal KUpr.
Se debe observar que el segundo criptograma representa para la tercera parte un identificador único que permite comprobar si este usuario ya ha visitado esta tercera parte.
En caso de que sí, los datos recogidos durante la visita precedente, así como los datos personales posibles de este usuario pueden utilizarse para personalizar presentación de la oferta de red.

[0055] En el caso que el segundo criptograma sea nuevo, significa que este usuario se conecta a la tercera parte por primera vez.
La tercera parte puede acceder el centro de confianza y puede transmitir el primer criptograma así como su propia identificación.
El centro de confianza puede desencriptar el primer criptograma para determinar de qué usuario se trata.
El centro de confianza puede devolver al tercero los datos personales de dicho usuario cuando el usuario ha autorizado esta transmisión y las reglas de compensación se cumplen.

[0056] En vez de claves asimétricas, las claves personales pueden ser una clave secreta simétrica.

[0057] Según una forma de realización de la invención, durante la inicialización de los datos personales con el centro de confianza, o en una fase posterior, el usuario puede recibir material criptográfico en forma de un certificado electrónico o un par de claves asimétricas.
Este material criptográfico se almacena en el dispositivo del usuario tal como un ordenador portátil, smartphone, tableta.
Este material se usa durante los pasos de autentificación realizados por el sitio web de la tercera parte.
Después de que el sitio web del tercero ha iniciado la conexión con el centro de confianza, los datos intercambiados entre el usuario y el centro de confianza se encriptan usando este material criptográfico.
Como consecuencia, el sitio web de la tercera parte no puede interferir en el procedimiento de autentificación y no puede entender los datos intercambiados.

[0058] Según otra forma de realización, un sitio web de una tercera parte puede enviar una solicitud para obtener datos personales de usuarios.
En esta solicitud, este sitio web puede definir su proposición respecto a la compensación por el acceso a los datos personales así como los criterios de búsqueda.
El centro de confianza buscará entonces en su base de datos los datos del usuario que corresponden con el criterio de búsqueda.
Una vez se ha encontrado un usuario, el centro verifica que las condiciones de acceso relacionadas con estos datos permiten la transmisión de estos datos.
Esta verificación puede tener en cuenta las condiciones de acceso generales tales como si esta categoría es accesible a terceros o si la tercera parte tiene permitido explícitamente el acceso a estos datos.

[0059] En ambos casos, el usuario puede definir criterios financieros para tener acceso a su datos y el centro de confianza compara las expectativas del usuario y la propuesta de la tercera parte.
Si se encuentra una correspondencia, los datos personales del usuario se transfieren al tercero y se realiza el crédito por la compensación ofrecida por la tercera parte.

[0060] En esta forma de realización particular de la invención, el sistema proporciona una posibilidad al usuario de monetizar la comunicación, bajo condiciones predefinidas, de ciertos de su datos personales a terceras partes que están dispuestas a compensarle por este tipo de comunicación.

[0061] Tales condiciones predefinidas pueden incluir el permiso para, o una denegación de permiso para, revender datos personales a terceras personas sujetas a los niveles de control mencionados anteriormente.

[0062] Para implementar el método de la invención, el centro de confianza tiene capacidades de tratamiento y de almacenamiento, así como medios de telecomunicación.
El centro de confianza está preferiblemente conectado a Internet de modo que los usuarios pueden colgar sus datos personales.
Las capacidades de tratamiento están a cargo de la protección de los datos personales, de organizarlos y de realizar la búsqueda solicitada por las terceras partes.

REIVINDICACIONES

1. Método para controlar el acceso a datos personales de un usuario (UT1, UT2) por un centro de confianza (TC) que comprende al menos una base de datos (TDB) que comprende, para un usuario específico, ubicaciones de memoria para datos personales, condiciones de acceso asociadas a los datos personales y datos de gestión,

- cargar por un usuario en la base de datos (TDB) del centro de confianza (TC) sus datos personales y asignar condiciones de acceso a dichos datos, donde dichos datos personales están divididos en al menos dos categorías con dos condiciones de acceso diferentes, donde cada categoría está asociada a un valor del usuario,
- solicitar acceso al centro de confianza (TC) por una tercera parte (TPWS) a los datos personales de una pluralidad de usuarios (UT), donde dicha solicitud comprende criterios de búsqueda,

caracterizado por el hecho de que los datos de gestión comprenden además al menos un contador,
y en caso de que la tercera parte no haya indicado un valor de la tercera parte:

- ejecutar por el centro de confianza (TC) el criterio de búsqueda sobre los datos personales de los usuarios para determinar un primer conjunto de usuarios que coincidien el criterio de búsqueda,
- devolver a la tercera parte (TPWS) información que muestra la cantidad del primer conjunto de usuarios que coinciden con el criterio, así como la suma del valor del usuario de cada usuario del primer conjunto,
- reconocer toda o parte de la suma por la tercera parte, definiendo así un segundo conjunto de usuarios que puede comprender todo o parte del primer conjunto,
- devolver los datos personales del segundo conjunto de usuarios para que la suma cubra los valores acumulados de los usuarios extraídos,

si no:

- dicha solicitud comprende además el valor de la tercera parte,
- ejecutar por el centro de confianza (TC) el criterio de búsqueda en los datos personales de los usuarios para determinar un segundo conjunto de usuarios que coinciden el criterio de búsqueda para el que el valor del usuario es igual o inferior al valor de la tercera parte,
- devolver los datos personales del segundo conjunto de usuarios,

y

- actualizar el contador del segundo conjunto de usuarios con el contenido del valor de sus respectivos datos personales.

2. Método según la reivindicación 1, donde la información que muestra la cantidad del primer conjunto de usuarios que coinciden con el criterio comprende los pasos de:

- agrupar todos los usuarios del primer conjunto de usuarios que tienen el mismo valor del usuario,
- transmitir a la tercera parte (TPWS), la cantidad de usuarios por grupo.

3. Método según la reivindicación 1, donde la tercera parte (TPWS) transmite un valor límite con su solicitud, y donde otro conjunto de usuarios es seleccionado de entre el segundo conjunto de usuarios de modo que la suma del valor del usuario de cada usuario del otro conjunto no exceda el valor límite.

4. Método según cualquiera de las reivindicaciones 1 a 3, donde la solicitud por la tercera parte (TPWS) comprende datos de filtración, el paso de transmitir los datos personales comprende un paso de filtración de los datos personales según los datos de filtración antes de la transmisión de éstos al sitio web de la tercera parte.

5. Método según cualquiera de las reivindicaciones 1 a 4, donde éste comprende los pasos de:

- verificar al menos algunos de los datos personales,
- asignar un valor del usuario diferente si los datos personales han sido verificados con éxito.

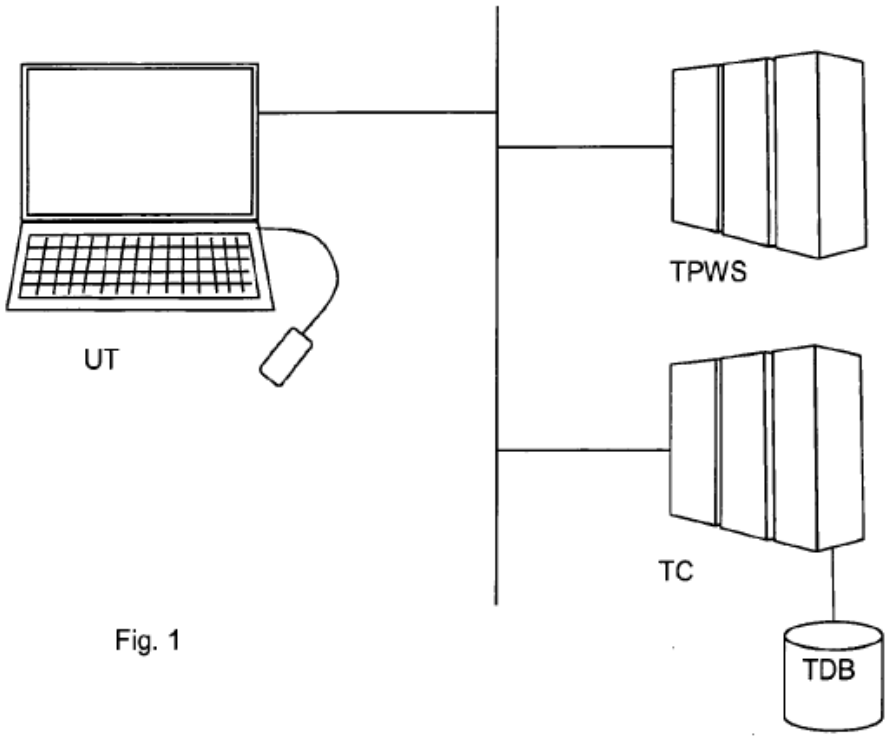

Fig. 1

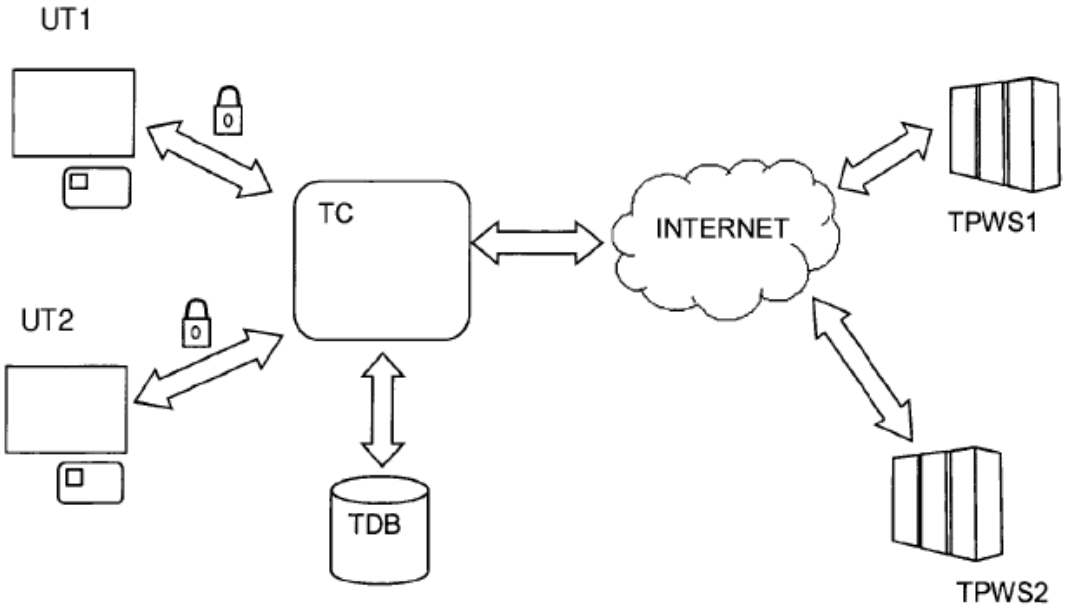

Fig. 2