(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 803 498**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.10.2012 E 12306353 (9)**

(97) Fecha y número de publicación de la concesión europea: **08.04.2020 EP 2728917**

(54) Título: **Proceso para proteger la privacidad de un usuario en una red**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.01.2021

(73) Titular/es:

ALCATEL LUCENT (100.0%)
Site Nokia Paris Saclay, Route de Villejust
91620 Nozay, FR

(72) Inventor/es:

KOSTADINOV, DIMITRE DAVIDOV;
BOUZID, MAKRAM y
AGHASARYAN, ARMEN

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Proceso para proteger la privacidad de un usuario en una red

La invención se refiere a un proceso para proteger la privacidad de un usuario en una red a la que dicho usuario está conectado a través de su terminal, tal como una aplicación que comprende medios para implementar dicho proceso y una arquitectura que comprende dicha aplicación.

La recopilación de datos personales sobre usuarios de servicios en una red está muy extendida, especialmente para estudios de inteligencia empresarial, encuestas sociales, encuestas de opinión o cualquier otro estudio para el que dichos usuarios no tengan que revelar su identidad. Para hacerlo, dichos servicios pueden requerir especialmente motores analíticos para recopilar y analizar datos personales de sus usuarios.

En particular, para proteger la privacidad de sus usuarios, los servicios generalmente eliminan del flujo de datos personales que podrían ser identificadores explícitos para dichos usuarios, tal como un nombre o apellido, un número de seguro social o una dirección IP (Protocolo de Internet), antes de entregar dicho flujo de fila a los motores analíticos.

Sin embargo, algunos de los datos personales de un usuario, incluso si no pueden considerarse a priori como identificadores explícitos, pueden usarse para identificar a dicho usuario cuando se combinan con otros datos personales. Dichas combinaciones pueden identificar notablemente a un usuario de manera única o permitir la identificación de dicho usuario entre un pequeño conjunto de usuarios potenciales con características equivalentes. Este puede ser el caso, por ejemplo, de la universidad donde se graduó dicho usuario, la nacionalidad o la empresa donde trabaja dicho usuario.

En consecuencia, un motor analítico malicioso que obtiene acceso a una combinación de dichos datos personales puede enviar consultas a fuentes de datos disponibles públicamente, tales como herramientas de búsqueda web, redes sociales u otras bases de datos públicas para obtener datos que son identificadores explícitos para el usuario. Además, la identificación de un usuario puede dar a dicho motor analítico malicioso acceso a información confidencial sobre dicho usuario que puede estar disponible entre los datos personales de dicho usuario, tal como sus elecciones de votación o sus eventuales enfermedades específicas.

Para proteger la privacidad de los usuarios, se han propuesto varias técnicas. Por ejemplo, hay algunas soluciones que aseguran a un usuario que los datos personales que envía a un servicio permitirán identificar al menos k usuarios (k es un número entero), especialmente de tal manera que sería difícil para un motor analítico identificar dicho usuario entre dichos k usuarios. Dicha solución se describe con más detalles en el artículo "Privacy Preserving Publishing on Multiple Quasi-Identifiers" (J. EPI, Y. TAO, J. LI, X. XIAO, 25ª Conferencia Internacional sobre Ingeniería de Datos, IEEE, páginas 1132-1135, 29 de marzo de 2009-2 de abril de 2009), en el que se garantiza el anonimato de un usuario al dividir las tablas en una base de datos para ocultar identificadores de dicho usuario. Además, esta solución tiene como objetivo minimizar la pérdida de información y mantener en orden los identificadores de otros k-1 usuarios (llamados "cuasi-identificadores") para permitir la recuperación de la base de datos inicial con cierta confusión según los requisitos de anonimato.

Otra solución conocida para proteger la privacidad de los usuarios se divulga en el artículo "Differential Privacy: A Survey of Results "(en "Theory and Applications of Models of Computation", C. DWORK, TAMC, Springer Verlag, abril de 2008). Esta solución tiene como objetivo evitar inferir información individual sobre un usuario mientras consulta un motor analítico que proporciona datos personales agregados. En particular, el motor analítico debe tomar el mismo tiempo de cálculo, incluso si no contiene los datos requeridos, y debe ser insensible a agregar o eliminar una sola fila.

Sin embargo, esta solución solo conserva la privacidad del usuario en el contexto del suministro de datos estadísticos, es decir, ya que todos los datos personales del usuario se almacenan en un motor analítico que proporciona dicho sistema estadístico. Por lo tanto, esta solución no puede garantizar realmente el anonimato del usuario por sí mismo, como, por ejemplo, durante la comunicación implícita entre dicho usuario y un motor analítico que requiere datos personales de dicho usuario para proporcionar datos estadísticos.

Otra solución común para proteger la privacidad del usuario consiste en anonimizar los datos de dicho usuario reemplazando los identificadores explícitos de dicho usuario por otros ficticios. Por ejemplo, dicha solución puede proporcionar el reemplazo de la columna "número de seguro social" en el perfil del usuario por una variable de incremento automático.

Sin embargo, esta solución también encuentra limitaciones, ya que los identificadores de los usuarios generalmente no se conocen de antemano, y a veces dichos usuarios ni siquiera son conscientes de que algunos datos que no son identificadores explícitos cuando se consideran por sí mismos se pueden recopilar para formar una combinación que puede identificarlos, así como identificadores explícitos.

La invención tiene como objetivo mejorar la técnica anterior al proponer un proceso que permita proteger la privacidad de los usuarios por sí misma cuando los motores analíticos requieren datos personales de dichos usuarios, asegurando

en particular que los datos personales de un usuario que se conocen como identificadores explícitos de dicho usuario nunca se comunican a dicho motor analítico.

Para ese fin, y de acuerdo con un primer aspecto, la invención se refiere a un proceso, llevado a cabo por una aplicación (3), para proteger la privacidad de un usuario en una red a la que dicho usuario está conectado a través de su terminal, siendo el proceso de acuerdo con la reivindicación 1.

Según un segundo aspecto, la invención se refiere a una aplicación para proteger la privacidad de un usuario de acuerdo con la reivindicación 6.

Otros aspectos y ventajas de la invención serán evidentes en la siguiente descripción hecha con referencia a la figura adjunta que representa una arquitectura que comprende medios para implementar un proceso de acuerdo con la invención.

En relación con esta figura, un proceso para proteger la privacidad de un usuario 1 en una red a la que dicho usuario está conectado a través de su terminal 2, tal como una aplicación 3 que comprende medios para implementar dicho proceso y una arquitectura para una red que comprende dicha aplicación 3, se describirá a continuación.

Como se representa, el terminal 2 del usuario 1 puede ser un ordenador personal, tal como un ordenador de escritorio o un ordenador portátil, o un terminal móvil tal como un teléfono inteligente.

El usuario 1 tiene notablemente un perfil que comprende datos personales de dicho usuario. Los datos personales comprenden identificadores explícitos de dicho usuario, es decir, datos que pueden permitir su propia identificación del usuario 1, tal como un nombre, un apellido, un número de seguridad social o una dirección IP. Los datos personales también comprenden otros tipos de datos que pueden ser comunes a varios usuarios, tal como una fecha de nacimiento, un lugar de nacimiento, una ciudad, una antigua universidad o un país, y, por lo tanto, no se pueden usar solos para identificar explícitamente al usuario 1.

La arquitectura comprende un módulo de construcción de perfil 4 que puede implementarse en el terminal 2, comprendiendo dicho módulo medios para construir el perfil del usuario 1. De manera conocida, el módulo de creación de perfiles 4 se puede adaptar para construir explícitamente el perfil enviando cuestionarios al usuario 1 para recopilar sus datos personales, así como para construir implícitamente dicho perfil basándose en los rastros de consumo de dicho usuario en la red.

El módulo de construcción de perfil 4 también comprende medios para almacenar el perfil del usuario 1. Tal como se representa, la aplicación 3 comprende una base de datos 5 para almacenar el perfil del usuario 1, interactuando el módulo de construcción de perfil 4 con dicha aplicación para almacenar dicho perfil en dicha base de datos.

Para garantizar una mejor privacidad al usuario 1, la aplicación 3 puede implementarse notablemente en el terminal 2 de dicho usuario.

Es obvio que los datos de identificadores explícitos no deben comunicarse de ninguna manera a los motores analíticos, ya que dichos motores requieren datos personales del usuario 1. Sin embargo, algunos otros datos personales que no se pueden utilizar por sí mismos para identificar al usuario 1 se pueden combinar con otros datos personales para permitir dicha identificación. Este puede ser el caso, por ejemplo, con el lugar de nacimiento, la fecha de nacimiento, la dirección actual o la antigua universidad del usuario 1.

Para evitar la comunicación de tales combinaciones peligrosas, el proceso proporciona el análisis del perfil del usuario 1 para crear un conjunto de posibles combinaciones de datos personales que sean susceptibles de permitir la identificación conjunta de dicho usuario. Por lo tanto, el proceso permite encontrar identificadores alternativos para el usuario 1. Para hacerlo, la aplicación 3 comprende un módulo administrador de descubrimiento 6 que comprende medios para analizar el perfil del usuario 1 para construir tales combinaciones. En particular, el módulo administrador de descubrimiento 6 interactúa con la base de datos 5 para analizar el perfil almacenado en dicha base de datos.

En particular, se pueden construir combinaciones de manera que el número de datos comprendidos en dichas combinaciones sea estrictamente menor que un límite superior predefinido, para evitar la explosión combinatoria del número de combinaciones posibles. De hecho, las combinaciones de alta complejidad, es decir, con un gran tamaño de datos, son menos probables de ser utilizadas por un motor analítico malicioso que las combinaciones más cortas.

Para evitar una explosión combinatoria de este tipo, el módulo administrador de descubrimiento 6 también se puede adaptar para interactuar con fuentes externas de información en la arquitectura, para identificar las dependencias entre los datos personales del usuario 1. Por ejemplo, si tanto una ciudad como un país están disponibles en el perfil del usuario 1 como datos personales sobre el lugar de nacimiento de dicho usuario, el módulo administrador de descubrimiento 6 puede adaptarse para considerar dichos datos como dependientes entre sí y para agruparlos durante la construcción de combinaciones.

El proceso además permite probar las combinaciones, para identificar entre las mismas las combinaciones que pueden permitir la identificación del usuario 1. Por lo tanto, el proceso proporciona la formulación de un conjunto de consultas correspondientes para cada una de las combinaciones construidas y el envío de dichas consultas a fuentes de datos 7 disponibles públicamente de la arquitectura. Para hacerlo, el módulo administrador de descubrimiento 6 comprende medios para formular las consultas y medios para enviar dichas consultas a las fuentes de datos 7.

Las fuentes de datos 7 disponibles públicamente pueden ser, por ejemplo, motores de búsqueda web, tal como Google®, o sitios de redes sociales dedicados, tales como Facebook®, Twitter @ o LinkedIn®.

El proceso además proporciona respuestas de análisis de las fuentes de datos 7 a sus consultas para verificar la presencia en dichas respuestas de identificadores explícitos de al menos k usuarios en la red, incluidos los identificadores explícitos del usuario 1, siendo k un número entero.

De hecho, algunas combinaciones de datos personales pueden dar lugar a respuestas con solo identificadores explícitos del usuario 1, por lo que estas combinaciones también pueden considerarse como identificadores explícitos de dichos usuarios. Pero la mayoría de las combinaciones pueden conducir a respuestas con identificadores explícitos de más de un usuario, ya que, por ejemplo, muchos usuarios pueden compartir el mismo lugar de nacimiento y la dirección actual.

Sin embargo, si las respuestas correspondientes a una combinación dada de datos personales comprenden muy pocos identificadores explícitos de diferentes usuarios, la privacidad del usuario 1 puede verse comprometida. Por lo tanto, el proceso también proporciona el almacenamiento de combinaciones cuyo conjunto correspondiente de consultas desencadena respuestas que contienen identificadores explícitos de menos de un número predefinido k de diferentes usuarios.

Para hacerlo, el módulo de administrador de descubrimiento 6 comprende medios para analizar las respuestas de las fuentes de datos 7 a las consultas para verificar la presencia en dichas respuestas de identificadores explícitos de al menos k usuarios, incluyendo identificadores explícitos del usuario 1, tales como medios para almacenar combinaciones cuyo conjunto correspondiente de consultas desencadenan respuestas que contienen identificadores explícitos de menos de k usuarios.

En particular, el proceso proporciona el análisis de las respuestas de las fuentes de datos 7 al comparar los datos personales contenidos en dichas respuestas con los datos personales que se identifican como identificadores explícitos en el perfil del usuario 1 y/o con los datos personales que se conocen como identificadores explícitos de otros usuarios de la red.

Para hacerlo, los medios para analizar el módulo de administrador de descubrimiento 6 está adaptado para hacer coincidir las respuestas con los datos personales del perfil del usuario 1 que está almacenado en la base de datos 5, para identificar en dichas respuestas los datos personales que se conocen como identificadores explícitos del usuario 1. Además, los medios para analizar el módulo de descubrimiento 6 están adaptados para interactuar con una base de datos de estadísticas de identificadores 8 de la arquitectura, en la que se almacenan identificadores explícitos de otros usuarios de la red, para verificar si los datos personales que están contenidos en las respuestas se conocen que son identificadores explícitos de dichos usuarios.

Por lo tanto, si las respuestas contienen identificadores explícitos verdaderos de menos de k usuarios, los medios para almacenar el módulo administrador de descubrimiento 6 almacenan las combinaciones de datos correspondientes como identificadores alternativos del usuario 1. Para hacerlo, la base de datos 5 puede adaptarse para almacenar tales combinaciones de identificadores alternativos, interactuando los medios para almacenar el módulo administrador de descubrimiento 6 con dicha base de datos para almacenar dichas combinaciones en dicha base de datos.

Además, para evitar una explosión combinatoria del número de posibles combinaciones de datos personales, el módulo de administrador de descubrimiento 6 se puede adaptar para detener cualquier análisis adicional en una combinación de datos que se ha identificado como identificador alternativo, ya que obviamente es inútil construir más superconjuntos combinaciones que incluyen una combinación tan relevante.

El proceso puede proporcionar que el número entero k sea configurado por el usuario 1. Para hacerlo, el módulo administrador de descubrimiento 6 comprende medios para permitir que el usuario 1 configure el entero k.

En particular, el proceso puede proporcionar la devolución al usuario 1 de las respuestas desde las fuentes de datos 7, de modo que dicho usuario valide o no el almacenamiento de las combinaciones de datos correspondientes de acuerdo con dichas respuestas, estando configurado el número entero k de acuerdo con dicha validación.

Para hacerlo, los medios para analizar el módulo administrador de descubrimiento 6 están adaptados para devolver al usuario 1 las respuestas desde las fuentes de datos 7 a un conjunto de consultas basadas en una combinación de datos determinada. El usuario 1 examinará las respuestas en su terminal 2, en particular, para verificar si dichas respuestas contienen un número suficiente de identificadores explícitos de otros usuarios diferentes. De hecho, el

usuario 1 puede, por ejemplo, usar diferentes apodos en diferentes fuentes de datos 7 y el módulo administrador de descubrimiento 6 puede considerar erróneamente dichos apodos como identificadores explícitos de otros usuarios, incluso si dichos apodos están todos vinculados al propio usuario 1.

Por lo tanto, si el usuario 1 considera que las respuestas devueltas no contienen suficientes identificadores explícitos diferentes, es decir, si el número de identificadores explícitos diferentes es demasiado pequeño, valida el almacenamiento de las combinaciones de datos que corresponden a dichas respuestas, por ejemplo, activando un botón interactivo dedicado que se muestra en su terminal 2 por los medios para analizar el módulo administrador de descubrimiento 6, de modo que los medios para almacenar almacenan dichas combinaciones en la base de datos 5 mientras que los medios para configurar configuran el número entero k, es decir, el número mínimo requerido de identificadores explícitos, de acuerdo con dicha validación.

Por lo tanto, el entero configurado k se memoriza como un umbral que los medios para analizar el módulo administrador de descubrimiento 6 se adaptarán para determinar si una combinación de datos es lo suficientemente segura o si dicha combinación debe almacenarse como un identificador alternativo del usuario 1. En particular, los medios para analizar se adaptarán para comparar con el número entero umbral k el número de identificadores explícitos diferentes contenidos en las respuestas de las fuentes de datos 7 que se activan indirectamente por la combinación de datos probados.

De acuerdo con otra realización, el entero k ya puede estar predefinido en los medios para configurar el módulo administrador de descubrimiento 6.

Una vez que se han detectado combinaciones de identificadores alternativos, el proceso proporciona la partición del perfil del usuario 1 en segmentos para separar en dicho perfil los datos personales que están comprendidos en dichas combinaciones almacenadas. Para hacerlo, la aplicación 3 comprende un módulo de segmentación de perfil 9 que comprende medios para dividir el perfil del usuario 1 en dichos segmentos.

En relación con la figura, el módulo de segmentación de perfil 9 interactúa con el módulo administrador de descubrimiento 6 y la base de datos 5 para obtener las combinaciones de datos que se han almacenado previamente como identificadores alternativos del usuario 1 y para dividir en segmentos el perfil de dicho usuario en consecuencia.

Para fines de optimización, el módulo de segmentación de perfil 9 se puede adaptar para almacenar en la base de datos 5 referencias a segmentos generados en lugar de dichos segmentos por sí mismos. De acuerdo con una variante, el módulo de segmentación de perfil 9 puede construir clases de equivalencia de datos personales y luego definir reglas para decidir qué datos personales de qué clases de equivalencia podrían proporcionarse en un mismo segmento. Por ejemplo, si una combinación de identificador alternativo contiene un país y un nombre de escuela como datos personales, entonces el módulo de segmentación de perfil 9 colocará la ciudad o la región de dicha escuela y dicho país en la misma clase de equivalencia del país, de modo que dicho módulo de segmentación nunca reunirá dicho país, dicha ciudad o dicha región en un mismo segmento.

Por lo tanto, como un motor analítico 10 envía una solicitud para recopilar datos personales del usuario 1, el proceso enviará a dicho motor analítico un segmento relevante del perfil de dicho usuario de acuerdo con dicha solicitud. Para hacerlo, la aplicación 3 comprende un módulo comunicador de perfil de preservación de la privacidad 11 que comprende medios para recibir la solicitud de dicho motor analítico 10, tal como medios para enviar a dicho motor analítico el segmento más relevante desde el módulo de segmentación de perfil 9 de acuerdo con la solicitud de dicho motor analítico.

En particular, la solicitud del motor analítico 10 comprende una especificación sobre el tipo de datos personales solicitados y/o la prioridad entre dichos datos solicitados. Por ejemplo, la solicitud puede referirse a la profesión, el país, el año de nacimiento y la educación del usuario 1, al tiempo que especifica que la profesión tiene una prioridad más alta que el nivel educativo.

El módulo comunicador de perfil de preservación de la privacidad 11 interactúa con el módulo de segmentación de perfil 9 y/o la base de datos 5 para identificar el segmento más relevante de acuerdo con la solicitud y envía dicho segmento al motor analítico 10. En particular, si el nivel educativo y la profesión se han separado previamente en diferentes segmentos porque forman juntos un identificador alternativo del usuario 1, el módulo de segmentación de perfil 9 enviará al módulo 11 un segmento que contiene solo la profesión, ya que dicho la profesión tiene una prioridad más alta que el nivel educativo, y el módulo 11 enviará dicho segmento con dicha profesión al motor analítico 10.

Por lo tanto, los datos personales del usuario 1 se comunican a los motores analíticos 10 sin correr el riesgo de que dichos motores analíticos recuperen identificadores explícitos de dicho usuario y, por lo tanto, descubran cualquier información personal confidencial de dicho usuario.

El proceso de la invención puede proteger la privacidad del usuario 1 con respecto a una gran categoría de motores analíticos 10. En particular, el proceso puede extenderse a proveedores de servicios en los que el usuario 1 se identifica con un apodo y no desea proporcionar su identidad real. De hecho, incluso si el usuario 1 usa un apodo,

también puede comunicar otros tipos de datos personales que se pueden combinar con otros datos para formar combinaciones alternativas de datos de identificación y dichas combinaciones pueden ser utilizadas por los motores analíticos 10 de dichos proveedores de servicios para encontrar el identidad del usuario al interactuar con otras fuentes de datos 7 en las que dicha identidad está disponible, tal como un sitio web personal o un perfil público de un sitio de red social tal como LinkedIn®, Twitter @ o Facebook®.

Por las razones mencionadas anteriormente, el proceso tiene beneficios obvios para el usuario 1, ya que dicho usuario tiene la garantía de comunicar sus datos personales a los motores analíticos 10 sin correr el riesgo de ser identificado, incluso indirectamente. Pero el proceso también presenta beneficios para tales motores analíticos 10, ya que los usuarios 1 serán menos reacios a proporcionarles sus datos personales. Por lo tanto, dichos motores analíticos 10 podrán recopilar más datos personales.

La descripción y dibujos ilustran meramente los principios de la invención. Por lo tanto, se apreciará que los expertos en la materia serán capaces de elaborar diversas disposiciones que, aunque no se describen o muestran explícitamente en este documento, incorporan los principios de la invención y se incluyen dentro de su espíritu y alcance. Adicionalmente, todos los ejemplos mencionados en el presente documento se conciben principal y expresamente para ser únicamente para fines pedagógicos para ayudar al lector en el entendimiento los principios de la invención y los conceptos contribuidos por el inventor o inventores para avanzar en la técnica, y deben interpretarse como sin limitación a tales ejemplos y condiciones específicamente mencionados. Además, todas las declaraciones en el presente documento que mencionan principios, aspectos y realizaciones de la invención, así como ejemplos específicos de la misma, pretenden abarcar equivalentes de los mismos.

REIVINDICACIONES

1. Proceso, realizado por una aplicación (3), para proteger la privacidad de un usuario (1) en una red a la que dicho usuario está conectado a través de su terminal (2), teniendo dicho usuario un perfil que comprende datos personales de dicho usuario, en donde los datos personales comprenden identificadores explícitos que pueden permitir por sí mismos la identificación del usuario y otros tipos de datos que no pueden usarse por sí mismos para identificar explícitamente al usuario,
proporcionándose dicho proceso para:

- analizar, mediante un módulo administrador de descubrimiento (6) de la aplicación (3), el perfil de dicho usuario para construir un conjunto de posibles combinaciones desde los otros tipos de datos que permiten la identificación explícita de dicho usuario;
- formular, mediante el módulo administrador de descubrimiento (6), un conjunto de consultas correspondientes para cada una de dichas combinaciones;
- enviar, mediante el módulo administrador de descubrimiento (6), dichas consultas a fuentes de datos (7) disponibles públicamente;
- analizar, mediante el módulo administrador de descubrimiento (6), respuestas desde dichas fuentes de datos a dichas consultas para verificar la presencia en dichas respuestas de identificadores explícitos de al menos k usuarios en la red, incluyendo identificadores explícitos de dicho usuario, siendo k un número entero;
- almacenar, mediante el módulo administrador de descubrimiento (6), como identificadores alternativos de dichas combinaciones de usuarios cuyo conjunto correspondiente de consultas desencadena respuestas que contienen identificadores explícitos de menos de k usuarios, incluyendo identificadores explícitos de dicho usuario
- dividir, mediante un módulo de segmentación de perfil (9) de la aplicación (3), las combinaciones de los identificadores alternativos en segmentos para separar los datos que se encuentran juntos en dichas combinaciones almacenadas;

recibir, mediante un módulo de comunicación de perfil de preservación de privacidad (11) de la aplicación (3), una solicitud desde un motor analítico (10) para recopilar datos personales de dicho usuario, en donde la solicitud comprende especificación sobre el tipo de datos personales solicitados y/o prioridad entre dichos datos solicitados;
identificar, mediante un módulo de comunicación de perfil de preservación de privacidad (11), un segmento que comprende datos con una prioridad más alta desde los segmentos de acuerdo con la solicitud, si los datos solicitados forman un identificador alternativo de dicho usuario que se ha separado en los segmentos; y
enviar, mediante un módulo de comunicación de perfil de preservación de privacidad (11), al motor analítico (10) el segmento que comprende datos con la máxima prioridad.

2. Proceso de acuerdo con la reivindicación 1, **caracterizado por que** se construyen combinaciones de manera que el número de datos comprendidos en dichas combinaciones es estrictamente menor que un límite superior predefinido.

3. Proceso de acuerdo con cualquiera de las reivindicaciones 1 o 2, **caracterizado por que** permite analizar las respuestas de las fuentes de datos (7) comparando los datos personales que están contenidos en dichas respuestas con los datos personales que se identifican como identificadores explícitos en el perfil del usuario (1) y/o a datos personales que se conocen como identificadores explícitos de otros usuarios en la red.

4. Proceso de acuerdo con cualquiera de las reivindicaciones 1 a 3, **caracterizado por que** el número entero k es configurado por el usuario (1).

5. Proceso de acuerdo con la reivindicación 4, **caracterizado por que** proporciona devolver al usuario (1) las respuestas desde las fuentes de datos (7), de modo que dicho usuario valida o no el almacenamiento de las combinaciones de datos correspondientes de acuerdo con dichas respuestas, configurándose el número entero k además de acuerdo con dicha validación.

6. Aplicación (3) para proteger la privacidad de un usuario (1) en una red a la que dicho usuario está conectado a través de su terminal (2), teniendo dicho usuario un perfil que comprende datos personales de dicho usuario, comprendiendo dicha aplicación:

- un módulo administrador de descubrimiento (6);
- un módulo de segmentación de perfil (9); y
- un módulo de comunicación de perfil de preservación de privacidad (11);

y en donde la aplicación está configurada para realizar los procesos de acuerdo con cualquier reivindicación anterior.

7. Aplicación (3) de acuerdo con la reivindicación 6, **caracterizada por que** comprende una base de datos (5) para almacenar el perfil del usuario (1) y para almacenar las combinaciones cuyo conjunto correspondiente de consultas desencadenan respuestas que contienen identificadores explícitos de menos de k usuarios.

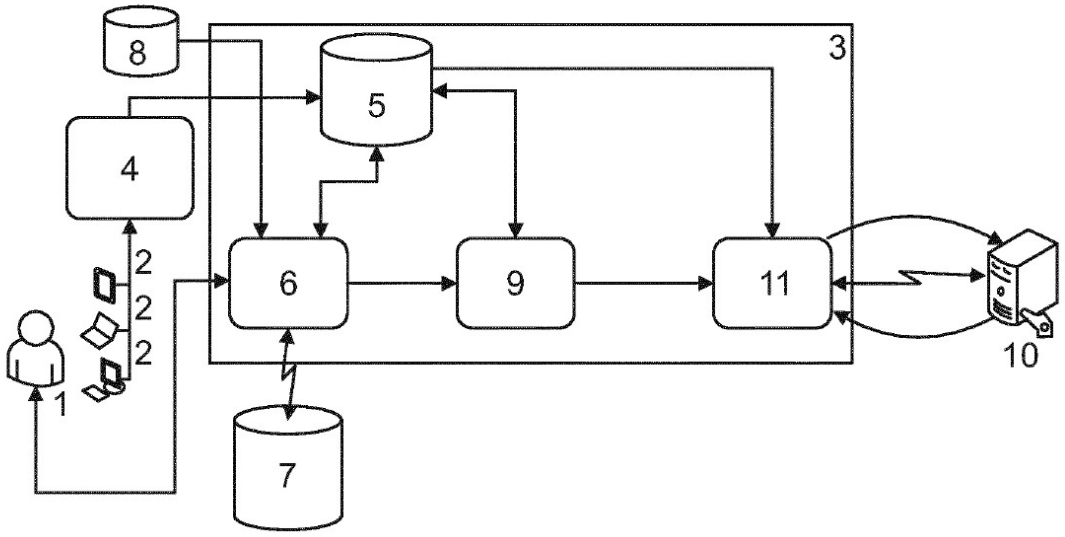

FIGURA ÚNICA