(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 972 041**

(51) Int. Cl.:

H04L 9/40 (2012.01)
G06F 21/62 (2013.01)
H04W 12/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.04.2020 PCT/EP2020/061821**

(87) Fecha y número de publicación internacional: **05.11.2020 WO20221778**

(96) Fecha de presentación y número de la solicitud europea: **29.04.2020 E 20724757 (8)**

(97) Fecha y número de publicación de la concesión europea: **03.01.2024 EP 3844934**

(54) Título: **Un sistema informático y método de operación del mismo para manejar datos anónimos**

(30) Prioridad:

29.04.2019 PT 2019115479

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.06.2024

(73) Titular/es:

MEDICEUS DADOS DE SAUDE S.A. (100.0%)
Estrada do Paço do Lumiar
1600 Lisboa - Carnide, PT

(72) Inventor/es:

VILLAX, PETER y
LOURA, RICARDO

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Un sistema informático y método de operación del mismo para manejar datos anónimos

Campo técnico

La presente solicitud está en el campo de los sistemas informáticos y la criptografía y se refiere a mejoras en la protección de identidad de usuario y derechos de privacidad a través del uso de arquitecturas de sistemas intrínsecamente seguras.

Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica beneficio y prioridad a la solicitud de patente portuguesa n.° 115.479, presentada el 29 de abril de 2019 y es una entrada de fase regional de la solicitud de patente internacional n.° PCT/EP2020061921, presentada el 29 de abril de 2020.

Antecedentes de la invención

Esta sección está destinada a proporcionar antecedentes o contexto a la invención que se menciona en las reivindicaciones y puede incluir conceptos que podrían perseguirse y son novedosos. A menos que quede claro por el contexto o se indique explícitamente como técnica anterior, tales divulgaciones no deben admitirse como técnica anterior a la descripción y reivindicaciones en la presente solicitud.

Internet ha permitido la creación de sistemas informáticos que manejan los datos personales de miles de millones de personas. Han llevado la era de la información desde el ámbito de las entidades corporativas y estatales hasta el nivel del individuo. Han permitido que las personas tengan un acceso sin precedentes a información que es útil para su trabajo, interacciones sociales y comercio, y a acciones que les permiten trabajar, interactuar y comerciar con facilidad, velocidad, comodidad y costes muy bajos. Las empresas basadas en Internet pueden proporcionar servicios a sus clientes a menudo sin coste para ellos, porque los datos que tales empresas recopilan de los clientes en interacciones conectadas a Internet informáticas tienen valor económico. Las preferencias y elecciones de los consumidores recopiladas durante estas interacciones e intercambios permiten a las empresas basadas en Internet crear perfiles de consumidores que les permiten dirigir con precisión ofertas comerciales a los consumidores incluidos en los perfiles definidos, reduciendo de esta manera los costes de segmentación, de comercialización y venta, e incluso para dirigir la oferta comercial al consumidor individual. Esto ha dado como resultado más opciones para el consumidor, precios más bajos y más volumen de ventas y, por lo tanto, es altamente beneficioso para la economía y la sociedad. Esto se logra por el ciudadano con acciones que no tienen coste - simplemente concediendo acceso a las empresas a sus datos personales.

Esta facilidad para identificar las preferencias del consumidor ha creado una segunda fuente de valor para las empresas, que va más allá de los ingresos obtenidos de la venta de productos y servicios convencionales, e incluye los ingresos de la venta de los datos personales de los consumidores a terceros que utilizan los datos para publicidad dirigida en Internet y aumentan sus ventas de productos y servicios convencionales.

La combinación de esta capacidad para dirigirse a mercados masivos con alta precisión se ha sofisticado además con el procesamiento de datos de consumidor personales combinados con datos del mundo físico. Recientemente, esta capacidad de combinar datos de múltiples fuentes se ha mejorado además con tecnologías que permiten al procesador de datos determinar patrones de comportamiento y elección y, a partir de ahí, predecir y, a veces, influir en las acciones de los ciudadanos, que por convención social y moral se consideran actos soberanos, libres de interferencias de terceros. A veces, los datos personales proporcionados por el ciudadano, de buena fe, a empresas basadas en Internet a cambio de servicios mejorados y beneficio económico se usan para propósitos encubiertos que no guardan relación con el propósito original y la intención para la que se proporcionaron los datos personales.

Sin embargo, en otras áreas, el miedo mismo al uso indebido de datos personales ha llevado al desarrollo subóptimo de los sistemas informáticos y al fallo en la obtención de beneficios para el ciudadano. Esto es particularmente visible en ciertos tipos de datos personales sensibles, tales como registros médicos y datos de salud, que se caracteriza por almacenarse en múltiples sistemas no interoperables desconectados donde la atomización de datos ha sido el mecanismo involuntario para la protección de datos personales. Los datos se distribuyen de manera redundante en tantos archivos, bases de datos y sistemas informáticos que pertenecen a múltiples proveedores de atención de la salud que, de hecho, es muy difícil, si no imposible, acceder al historial clínico completo de un paciente. Recopilar datos de atención de la salud personales y consolidarlos en un único sistema tendría un interés público significativo.

Por lo tanto, existe una necesidad importante de mejorar la forma en que los sistemas informáticos tratan los datos personales, evitando situaciones donde se abusa, o abordando otras en las que se infrautilizan. Tal es la invención que se presenta en este punto y aborda un problema que tiene sus raíces en una deficiencia tecnológica característica de Internet, que es la incapacidad, hasta ahora, para usar los datos personales de forma segura y consentida, donde el ciudadano tiene el control y sus derechos de privacidad están protegidos. Resolver este problema de control

idealmente no alteraría el protocolo de comunicaciones de Internet, lo que no sería práctico y, de hecho, no es necesario, sino estableciendo un nuevo modelo de relación entre sus diversos participantes y colocando al individuo como la parte controladora en las interacciones de Internet, a través de su dispositivo informático personal.

La solución indicada por la presente invención se basa en la necesidad de anonimización y cifrado de registro de datos. La protección de datos personales en Internet, datos particularmente sensibles, tales como datos personales de salud o cualquier otro tipo de datos que el propietario desee mantener reservados, confidenciales o secretos es importante y se han desarrollado varios métodos para lograr este propósito. Uno de tales métodos implica la anonimización que oculta la identidad del propietario y la anonimización irreversible, lo que hace imposible la reidentificación. En aplicaciones donde es útil mantener un sujeto de datos anónimo, pero mantener la capacidad de agregar datos bajo un término de identificación, se puede usar un identificador anónimo que tiene una relación de uno a uno con el propietario. De esta manera, los datos que pertenecen a la misma persona pueden almacenarse, organizarse y procesarse bajo la clave de identificador anónimo del propietario.

También se debe tener cuidado para evitar sistemas informáticos y aplicaciones informáticas que tengan acceso a medios de reidentificación y una forma técnica de hacerlo es usando estos identificadores anónimos informáticos que no conllevan relación con el nombre original o identificadores personales, tal como la fecha de nacimiento del propietario, dirección o números de identificación personal, por ejemplo. Además, particularmente en el caso de ordenadores conectados a redes muy grandes tales como Internet y con la posibilidad de acceso público, para almacenar y comunicar los datos en texto sin formato, es decir, inmediatamente legible y comprensible por cualquier parte, es un riesgo para la privacidad. El uso de métodos criptográficos es una solución útil al problema y puede usarse para proteger información sensible de interés tal como registros de compra, registros médicos, registros financieros, registros de impuestos, registros de propiedad, preferencias del consumidor, etc., que se procesan en estos sistemas informáticos en red.

Usando estas técnicas, es necesario que, incluso si los identificadores personales del sujeto de datos están cifrados y la información de interés se anonimiza, la información de interés no contiene datos que puedan permitir inferir la identidad del sujeto de datos, haciendo coincidir esos datos de texto sin formato con otras bases de datos donde se incluyen datos de interés similares y se conoce la identidad del sujeto. Por lo tanto, parece que una forma eficaz de asegurar los derechos de privacidad del sujeto de datos es simplemente ocultar su identidad. Para ocultarlo completamente, incluso podría ser útil eliminar el método de verificación de identidad de nombre de usuario / contraseña convencional, que para funcionar puede requerir que un ordenador conozca el nombre de usuario del sujeto de datos y almacene su contraseña.

Sin embargo, hay varias aplicaciones donde existe la necesidad de revertir la anonimización de los datos personales del propietario. Tales aplicaciones incluyen la atención de salud, cuando sea necesario volver a identificar al propietario, por ejemplo, cuando es deseable cambiar el tratamiento médico y, por lo tanto, identificar positivamente al paciente. Además de la atención de la salud, hay otras situaciones donde es necesario revertir la anonimización del propietario, y esto incluye todas las situaciones en las que el propietario necesita o desea ser contactado por el proveedor de datos o servicios - para probar la propiedad de los recursos, para recibir información sobre facturas a pagar, cambios en los términos y condiciones, información de producto, la oferta de nuevos servicios, la solicitud de consentimiento, etc.

La anonimización reversible se conoce como seudonimización, que se define en el Reglamento General de Protección de Datos de la Unión Europea como el procesamiento de datos personales de tal manera que los datos personales ya no pueden atribuirse a un sujeto de datos específico sin el uso de información adicional. Una implementación práctica de esto es configurar un sistema informático para seleccionar un registro de datos que contenga información de interés relacionada con su propietario de sujeto de datos, identificado con un código confidencial donde el código también se almacena en una ubicación de archivo diferente del mismo ordenador u otro ordenador, que contiene también el nombre del sujeto de datos y los identificadores personales. Al hacer coincidir la información en ambos archivos, el sujeto de datos puede volver a identificarse. De esta manera, el archivo informático que contiene los registros de salud seudonimizados u otra información sensible de varios sujetos de datos puede procesarse sin que se muestre su identidad, pero cuando surge la necesidad, cada registro de datos puede rastrearse hasta la identidad del sujeto de datos por medio del segundo archivo de datos.

Desafortunadamente, esta división de datos donde la identidad real del sujeto de datos se mantiene separada en otro archivo informático es propensa al abuso, particularmente cuando ambos archivos están bajo el control del mismo servidor informático de controlador de datos, el servidor informático operado por una entidad que, entre otras actividades, usa sus sistemas informáticos para procesar datos que pertenecen a un sujeto de datos y que se originan en el ordenador del sujeto de datos. A menos que se evite absolutamente el abuso intencional o la reidentificación accidental configurando apropiadamente todos los ordenadores implicados, siempre existe el riesgo de que se produzca una brecha de datos y los datos personales se vean comprometidos y se usen para propósitos que el sujeto de datos no consintió originalmente, ya sea explícita o implícitamente. Por este motivo, existe la necesidad de que los servidores informáticos de controlador de datos se configuren para evitar que los operadores internos, ya sea por accidente o con intención, o que operadores externos malintencionados reviertan un identificador seudonimizado, pero tal configuración no debería impedir que el servidor informático de controlador de datos pueda establecer

comunicación con el ordenador de sujeto de datos para transmitir e intercambiar los datos del sujeto.

La presente solicitud presenta una solución a esta paradoja y describe un sistema informático seguro y un método donde el ordenador del sujeto de datos está configurado para generar un identificador anónimo usado para ocultar la identidad de nombre del sujeto de datos y los identificadores personales, evitando por tanto que tales datos de identificación se transmitan al servidor informático de controlador de datos y, por lo tanto, haciéndolos insensibles a la liberación accidental o brecha maliciosa. El ordenador del sujeto de datos está configurado además para permitir que el sujeto de datos indique su consentimiento en cuanto a si sus datos personales pueden transferirse, a quién, para qué usos y durante cuánto tiempo, y para establecer comunicación con el servidor informático de controlador de datos, de tal manera que el servidor informático de controlador de datos pueda verificar la identidad del ordenador del sujeto de datos.

Hay varias referencias en la bibliografía a modelos de anonimización variable que permiten que una medida de datos personales sea conocida o descubrible.

La solicitud de patente WO/2018/201009 describe sistemas y métodos que logran un propósito similar al de la presente solicitud, pero lo hace a través del uso de un identificador dinámico para cada usuario. Los identificadores dinámicos son muy eficientes en términos de anonimización de usuarios, pero plantean la cuestión de la responsabilidad legal en cuanto a qué entidad es responsable de atribuir el identificador a un usuario, gestionar el cambio dinámico del identificador y garantizar que el identificador cambiado dinámicamente siempre se refiere a la misma persona. Los identificadores estáticos, severamente protegidos, y los métodos de minimización de datos pueden ofrecer un mejor compromiso entre seguridad, operatividad y garantías legales.

La publicación de solicitud de patente de Estados Unidos 2015/0149208 describe un sistema para recopilar y anonimizar datos de salud de múltiples proveedores de atención de la salud donde el enfoque está en mejorar la confianza de que el identificador anónimo siempre se refiere a la misma persona.

La publicación de solicitud de patente de Estados Unidos 2002/0091650 describe un sistema que proporciona a los profesionales del marketing información confidencial acerca de las elecciones de los consumidores al proporcionar una comprensión clara de los clientes como grupo o como subgrupos específicos en términos de geografía, estilos de vida, hábitos de compra, mientras se protege su privacidad e identidad. Sin embargo, la solución presentada no es capaz de llegar a individuos específicos.

La patente de Estados Unidos 8234698 describe un sistema donde un sujeto de datos puede acceder a servicios web de una manera que aún permite que el proveedor de servicios web identifique positivamente al cliente, es decir, para pago seguro de una suscripción o una transacción, mientras que impide el acceso a los identificadores personales del cliente. Esto se hace a través de una autoridad de certificación anónima de terceros, así como la autenticación cara a cara por una organización confiable, tal como un banco o una sociedad de valores. Este es un procedimiento complejo y costoso.

La patente de Estados Unidos 7840813 y la publicación de solicitud de patente de Estados Unidos 2010/0131765 ambas incluyen algunas de las características del caso anterior, pero específicamente permiten la revocación o reversión del anonimato, contrariamente al objetivo de la presente solicitud donde el anonimato es deseablemente irreversible y donde la reversibilidad, cuando sea posible, está fuera del control del controlador de datos.

La publicación de solicitud de patente de Estados Unidos 2014/0372149 intenta reconciliar la necesidad de anonimización de los datos personales del paciente mientras que proporciona acceso a los datos de salud del paciente sin ambigüedad, por medio del almacenamiento de registros de paciente que se almacenan en la nube, con campos de identificación anonimizados para un acceso seguro de los registros de paciente por múltiples médicos. Estos registros de paciente, principalmente imágenes, se acceden en la pantalla de visualización principal a través de un ordenador de autorización operado por el médico asignado del paciente. Este ordenador contiene datos predefinidos acerca de los pacientes cuyos datos han de inspeccionarse por el médico y únicamente se visualizan registros de paciente que coinciden con los datos predefinidos. Sin embargo, los servidores informáticos de controlador y de procesador de datos contienen tanto los registros de paciente como los datos de identificación del paciente y, por lo tanto, pueden programarse para hacer coincidir los primeros con los últimos y, por lo tanto, reidentificar al paciente.

La patente de Estados Unidos 8.635.464 detalla un método completo para cifrar un sistema informático, pero uno donde una autoridad de certificación y revocación y el sujeto de datos son entidades separadas. En este punto, el sujeto de datos no tiene el control de la gestión de sus códigos de cifrado y no está en posición de tener el control exclusivo del acceso a sus datos personales.

La patente de Estados Unidos 5.369.702 describe un sistema de cifrado multimedia de múltiples niveles en el que el objeto cifrado se etiqueta con un código que determina si el receptor del mensaje cifrado está autorizado para descifrarlo. Este sistema emplea cifrado anidado para que el mismo mensaje pueda transmitirse del emisor al receptor al receptor en una cadena de transmisión, pero el acceso será selectivo dependiendo de si el receptor es un lector autorizado según se especifica por la etiqueta. La invención se refiere a la distribución de información a un gran número

de personas, donde existe la necesidad de dar acceso de manera selectiva basándose en los niveles de autorización de los receptores.

La patente de Estados Unidos 9.910.902 describe un proceso para anonimizar la información identificable de usuario, pero que no oculte completamente al ordenador de procesador de datos la identidad del sujeto de datos, ya que el procesador mantiene tablas de mapeo de anonimización que le permiten volver a identificar al sujeto de datos.

La solicitud de patente de Estados Unidos US 2016/147945 A1 describe un método y sistema para buscar y obtener datos de atención de la salud de paciente relacionados con un sujeto de datos de uno o más servidores informáticos proveedores de datos. Los identificadores personales del paciente no se divulgan mientras se transfieren los datos de interés desde los servidores informáticos proveedores de datos a un servidor informático de controlador de datos confiable. Los datos de interés están vinculados a identificadores personales del sujeto de datos correspondiente en el servidor informático de controlador de datos confiable y, por lo tanto, no se manejan ni almacenan en una forma anonimizada en el servidor informático de controlador de datos confiable.

La solicitud de patente de Estados Unidos US 2007/192139 A1 describe sistemas y métodos de búsqueda, obtención y reidentificación de datos de atención de la salud de pacientes relacionados con un sujeto de datos. Se usa un identificador anonimizado cifrado para obtener un identificador de paciente asociado con datos de interés relacionados con un sujeto de datos. Los datos de interés relacionados con un sujeto de datos se transfieren desde servidores informáticos proveedores de datos a un servidor informático de controlador de datos confiable en una forma anonimizada. El sujeto de datos no tiene el control de la transmisión de los correspondientes datos de interés al servidor informático de controlador de datos confiable. Los datos de interés no se devuelven al sujeto de datos desde el servidor informático de controlador de datos confiable.

La solicitud de patente de Estados Unidos US 2017/372096 A1 describe sistemas y métodos para transferir datos de interés relacionados con un sujeto de datos desde un primer servidor en una primera región a un segundo servidor en una segunda región en una forma anónima. Los datos de interés se almacenan en el primer servidor junto con identificadores personales que identifican a los sujetos de datos. Los identificadores personales se eliminan de los datos de interés y los datos de interés se transmiten junto con un identificador anónimo al segundo servidor para llevar a cabo análisis de datos en el segundo servidor. Los datos analizados se transmiten de vuelta desde el segundo servidor al primer servidor, reidentificados con identificadores personales basándose en el identificador anónimo en el primer servidor y almacenados en el primer servidor. El sujeto de datos no tiene el control de la transmisión de los correspondientes datos de interés al servidor informático de controlador de datos confiable.

Por lo tanto, existen varios casos de la técnica anterior en los que se han usado sistemas de verificación, cifrado y gestión de derechos de acceso para proteger datos personales. Sin embargo, ninguno de ellos ha colocado al sujeto de datos ciudadano en el centro del modelo de protección, con la facultad plena y exclusiva de conceder y revocar el acceso a sus datos personales, con anonimización y con la posibilidad de mantener una comunicación cifrada con la parte que gestiona y procesa los datos personales anonimizados del sujeto de datos.

Ahora hemos desarrollado un sistema informático único y un método para usarlo para permitir el procesamiento y la comunicación de datos seguros, proporcionando simultáneamente tal acceso y prevención de acceso, de una manera que es controlada automáticamente por el sujeto de datos a través de su ordenador, usando herramientas a su disposición y sin necesidad de conocimientos especiales.

La invención es útil en cualquier campo donde se almacenan datos personales en un sistema informático y exista una necesidad de proteger la privacidad del sujeto de datos o propietario de datos. Una lista de posibles campos sensibles incluye estudios científicos o no científicos, recopilaciones de datos y extracciones de datos donde la información de interés puede incluir el género, orientación sexual, raza, datos médicos y de atención, datos genéticos, antecedentes penales, datos biométricos, comportamiento, estilo de vida, capacidad, religión, creencias, opciones políticas, afiliación de partidos, afiliación sindical, formulación de políticas, sondeos y encuestas de opinión, respuestas a publicidad, grupos de discusión, reclutamiento de recursos humanos, gestión empresarial, gustos de los consumidores y decisiones de compra, registros e historial de compras, registros e historial de impuestos, inversiones y decisiones para invertir o ahorrar, gustos y no gustos, relaciones sociales, etc. De hecho, áreas tan sensibles que algunas jurisdicciones prohíben su procesamiento predeterminado, permitiéndolas únicamente bajo excepciones justificadas. La presente invención permite que se investiguen tales campos sensibles con el respeto más estricto de los derechos de privacidad de los individuos y se reivindica la protección para todos los campos aplicables.

Sumario de la invención

Entidades de la invención. Al presentar la invención, ahora se hará referencia a los diversos participantes y funciones presentes en este sistema informático de intercambio y procesamiento de datos personales seguro.

La presente invención identifica tres categorías de participantes y sus respectivos sistemas informáticos. En la primera categoría, los sujetos de datos o sujetos son las personas o entidades individuales que usan ordenadores para procesar datos, incluyendo datos personales. Son ciudadanos, consumidores, profesionales, reclutadores, gestores,

contribuyentes, pacientes, empresas, organizaciones, organizaciones sin ánimo de lucro, organizaciones no gubernamentales, estados, expertos en inteligencia, los militares, denunciantes, creyentes, votantes, viajeros, escritores, fotógrafos, artistas, amigos, inversores, ahorradores, etc., de hecho, personas o entidades en cualquier función donde se generan datos como resultado de la actividad humana. Los datos producidos por máquinas tales como sensores de monitorización también se incluyen en este alcance y el sujeto de datos será la persona o entidad que ha originado los datos. La propiedad legal real puede variar de acuerdo con la jurisdicción, pero, para los propósitos de la presente solicitud, "sujeto de datos" se refiere a la persona o entidad que generó originalmente los datos informáticos o en cuyo nombre se generaron. Una característica valiosa de estos datos es que cuando se generan en escalas muy grandes, es posible extraer nueva información y analizar correlaciones, causas y efectos y patrones de rendimiento, comportamiento o elecciones. El uso de ordenadores es necesario para todas tales operaciones, pero, en general, no están preparados para dar a los sujetos de datos una protección adecuada para sus derechos de privacidad.

En la segunda categoría, los controladores de datos son personas o entidades que usan sistemas informáticos y son legalmente responsables de las operaciones de procesamiento de datos, incluso si las subcontratan a procesadores de datos especializados. Algunos controladores de datos obtienen un beneficio económico del acceso a la información de los sujetos de datos, como un objetivo comercial principal o estratégico. Tales controladores de datos incluyen actualmente a) plataformas de motor de búsqueda de Internet, que registran los intereses de los sujetos de datos; b) plataformas comerciales y de negocios en Internet, que almacenan datos y pueden crear mercados para consumidores y proveedores de bienes y servicios; y c) redes sociales de Internet, que registran y ayudan a gestionar la interacción social y la comunicación entre personas. Los tres grupos de este tipo registran la información de los sujetos de datos sobre búsquedas de datos, compras e interacciones sociales para obtener un perfil de consumidor preciso de cada individuo y pueden usar esa información y datos de perfil para vender servicios de publicidad e información y medios de orientación de consumidor precisos. En este caso, los sujetos de datos se benefician ofreciéndoles servicios gratuitos de alto valor y comodidad, mientras que los controladores de datos convierten los datos gratuitos de los sujetos en un negocio rentable.

La presente solicitud crea un nuevo tipo de servidor informático de controlador de datos, que accede, recupera y consolida datos de sujeto de cualquier fuente donde pueda ubicarse y los usa de una manera que es consistente con la protección de los derechos de privacidad y autodeterminación del ciudadano. Este controlador de datos será seleccionado por el sujeto de datos para llevar a cabo, en nombre del sujeto, toda tal extracción de datos, consolidación, almacenamiento y procesamiento mientras se aseguran los derechos de privacidad. En la presente invención, esta entidad se denomina controlador de datos confiable y opera el servidor informático de controlador de datos confiable. El servidor informático de controlador de datos confiable está configurado, como parte del sistema informático descrito en la presente invención, para procesar datos personales de una manera que proteja los derechos de privacidad de los sujetos de datos.

La tercera categoría de participante es el proveedor de datos. Hay muchas entidades corporativas donde el negocio principal es proporcionar servicios o vender bienes, pero, que en el proceso de realizar su actividad principal adquieren o generan cantidades muy grandes de datos personales valiosos a través del uso de sistemas informáticos. Los ejemplos incluyen los proveedores de datos mencionados anteriormente, bancos, compañías de seguros, contables, asesores fiscales, empresas financieras, empresas de marketing, empresas de encuestas a consumidores, compañías farmacéuticas, organizaciones de investigación por contrato, organizaciones no gubernamentales, servicios nacionales de salud, organizaciones censales, empresas de encuestas de opinión pública, hospitales, consultorios médicos, empresas de servicios de ensayos clínicos, etc. De hecho, cada vez más, la línea se difumina entre aquellas empresas donde los datos son el negocio principal y las empresas de servicios y productos donde la importancia de los datos está creciendo, en ocasiones más allá de la importancia del negocio original. Lo que caracteriza a este último grupo es que sus sistemas informáticos contienen grandes conjuntos de datos de información personal y pueden tener interés en aprovecharlos económicamente contratando con un controlador de datos especializado. Configurar servidores informáticos proveedores de datos para operar de una manera que asegure la protección de derechos de privacidad de sujetos de datos es una parte de esta invención.

Ciertos tipos de proveedor de datos son particularmente importantes en la presente invención. El proveedor de atención de la salud es un tipo de proveedor de este tipo e incluye médicos, farmacéuticos, enfermeras y cualquier personal que esté autorizado a consultar los registros clínicos del sujeto para el propósito de tratamiento y al mismo tiempo añadir nueva información de tratamiento y de salud. En este punto, existe la necesidad de que el servidor informático del proveedor de atención de la salud pueda identificar positivamente al sujeto de datos como paciente, para asegurarse de que los registros médicos subyacentes pertenecen de hecho al paciente que se está observando y tratando, pero este acceso no debe comprometer la privacidad de la información del sujeto de datos.

Una cuarta categoría opcional de participante es el proveedor de verificación de identidad, donde un servidor informático verifica la identidad del sujeto de datos de modo que pueda confirmarse la identidad de la persona. En una realización en línea, el proveedor de verificación de identidad es un servidor informático configurado para acceder y conectarse a servidores informáticos que gestionan bases de datos muy grandes que almacenan información de ciudadanos y específicamente datos de identificación, tal como el nombre, identificadores personales y, lo que es importante para la presente solicitud, una dirección electrónica, una dirección de correo electrónico o un número

asociado con el teléfono inteligente o tableta del sujeto de datos o cualquier otro dispositivo informático personal con capacidades de comunicación. Ejemplos son bases de datos gubernamentales de agencias de permisos de conducción o autoridades fiscales y bases de datos privadas de operadores de telefonía celular.

Los identificadores personales son elementos de información que pueden usarse para identificar al sujeto de datos e incluyen el nombre de la persona, sexo, fecha de nacimiento, dirección, cualquier número de identificación personal (tarjeta de identidad, número de identificación fiscal, número de seguro social, número nacional de salud, número de titular de la póliza de seguro, número de cuenta bancaria, número de teléfono, número de teléfono celular, etc.) o direcciones personales (dirección de residencia, dirección del empleador, nombre de usuario, nombre de red social, dirección de correo electrónico, dirección de sitio web, nombre de ordenador y dirección electrónica, etc.), todos conocidos colectivamente como identificadores personales. En la medida en que los miembros de la familia también puedan ayudar a identificar a una persona, los identificadores personales de los miembros de la familia también se incluyen en el perímetro de los identificadores personales de una persona.

Las realizaciones de la presente invención usan tecnología de cifrado. El cifrado es el mecanismo de manipulación de datos usado por un ordenador del sujeto de datos o un servidor informático de controlador de datos para cifrar un mensaje de modo que, durante la transmisión, un ordenador de terceros no puede entenderlo, seguido por el uso de un mecanismo estrechamente relacionado por el receptor para revertir el proceso de manipulación del mensaje, descifrarlo y obtener acceso de lectura a su contenido. Los métodos de cifrado también incluyen la capacidad de confirmar las identidades del sujeto de datos y el receptor y la capacidad de identificar cualquier cambio en los datos cifrados y garantizar la integridad de su contenido.

El cifrado requiere claves criptográficas informáticas. Una clave es una secuencia de letras, números o bytes de información que son manipulados por un algoritmo de codificación en el lado del emisor informático para transformar texto o datos legibles en series de signos o caracteres ininteligibles. La clave se usa a continuación por el ordenador de recepción del texto codificado para descifrar el mensaje de vuelta a texto sin formato.

Cuatro tipos de sistemas criptográficos informáticos son importantes en la presente invención.

En el primer tipo, el ordenador de envío y el ordenador de recepción usan la misma clave criptográfica y el mismo algoritmo de codificación. Esto se conoce como criptografía de clave simétrica y es un sistema de codificación relativamente rápido en términos de recursos informáticos. Una dificultad en este punto es gestionar el acceso a esta clave única y esto hace que sea más apropiado codificar comunicaciones entre solo dos ordenadores - una clave simétrica para cada par de ordenadores de envío y recepción.

El cifrado de clave simétrica informática usa una única clave k tanto para el cifrado como para el descifrado informático. Hay muchos tipos diferentes de cifrado de clave simétrica informática. Un ejemplo es la Norma de Cifrado Avanzado ("AES"). En general, el cifrado de clave simétrica informático emplea una serie de operaciones deterministas para el cifrado que pueden invertirse para el descifrado. Para el cifrado de clave simétrica informático, la clave de cifrado generalmente se mantiene en secreto por ambos ordenadores de comunicación ya que el acceso a la clave permite que tenga lugar el descifrado.

En el segundo tipo de sistema criptográfico informático, conocido como criptografía de clave asimétrica, el ordenador de envío y el ordenador de recepción usan un par de claves criptográficas diferentes, una clave pública y una clave privada. La criptografía de clave pública/clave privada informática se usa ampliamente en transacciones comerciales y protocolos de intercambio de información. Un sistema criptográfico de clave pública/clave privada generalizado se denomina la técnica criptográfica "RSA", donde RSA incluye las primeras letras de los apellidos de los inventores del método: Rivest, Shamir y Adleman. En este sistema criptográfico informático, se generan pares de claves criptográficas. En general, la clave criptográfica pública se distribuye públicamente y se denomina "clave pública", mientras que, la clave criptográfica privada se mantiene en secreto por el ordenador que recibe el mensaje cifrado y se denomina "clave privada" o "clave secreta". En uso normal, el ordenador de envío del mensaje lo codificará usando la clave pública del ordenador de recepción, que es generalmente conocida, y se decodificará por el ordenador de recepción usando su clave privada, que es confidencial.

También pueden usarse métodos criptográficos de clave asimétrica para firmar digitalmente un mensaje para proporcionar autenticación de mensaje entre ordenadores. En un ejemplo, el mensaje a firmar consiste en la clave pública del emisor. El ordenador de envío cifrará el mensaje usando la clave privada del emisor y enviará el mensaje cifrado al ordenador de recepción. El ordenador de recepción descifrará el mensaje usando la clave pública conocida del ordenador de envío. Si el contenido del mensaje descifrado es igual a la clave pública del ordenador de envío, la firma digital se ha verificado con éxito. Para firmar digitalmente mensajes más largos, es útil hacer la función de troceo de todo el mensaje en primer lugar, cifrarla con la clave privada del emisor y, a continuación, transmitirla al ordenador de recepción para su descifrado y verificación. Hay varios métodos disponibles, el método preferido en este punto es el algoritmo de firma digital de curva elíptica (ECDSA), una variante de RSA.

Un tercer tipo de criptografía informática útil es la cadena de bloques. Este es un sistema seguro para registrar transacciones que se distribuye en un gran número de nodos de procesamiento, tan grande que derrotar el cifrado no

es viable. Cada objeto de información que se cifra usando la cadena de bloques normalmente contiene una función de troceo criptográfica del bloque anterior, una indicación de tiempo y datos de transacción. Por diseño, una cadena de bloques es intrínsecamente resistente a la modificación de los datos. Es un libro mayor informático distribuido abierto que puede registrar transacciones entre dos ordenadores de manera eficiente y de una manera verificable y permanente. Para su uso como un libro mayor distribuido, una cadena de bloques se gestiona típicamente por una red informática entre pares que se adhiere colectivamente a un protocolo para la comunicación entre nodos y la validación de nuevos bloques. Una vez registrados, los datos en cualquier bloque dado no pueden alterarse retroactivamente sin la alteración de todos los bloques posteriores, lo que requiere la colusión de la mayoría de la red.

En la presente solicitud, la cadena de bloques puede ser útil para registrar transacciones de información entre los ordenadores de los sujetos de datos, verificadores de identidad, proveedores de datos y el controlador de datos confiable, así como dar al sujeto de datos la posibilidad de adaptar el consentimiento y los derechos de visualización para sus datos personales mediante el uso de contratos inteligentes, una característica de la cadena de bloques. Los contratos inteligentes permiten que el sujeto de datos especifique a través de su ordenador quién y de quién pueden ver los datos personales y los datos de interés, qué categorías de datos pueden verse y por quién, que puede escribirse y por quién, qué acciones se pueden autorizar dependiendo de los datos subyacentes de interés, y para conceder o eliminar global o selectivamente el consentimiento y los derechos de acceso informáticos.

Un cuarto método criptográfico es el algoritmo de troceo seguro, tal como SHA-256, SHA-512 o cualquiera de sus sucesores. Este es una función matemática ampliamente usada que cifra una expresión en una versión cifrada con un mayor nivel de seguridad que las claves asimétricas. En el estado de la técnica actual, los ataques de fuerza bruta para revertir un número con función de troceo tardan significativamente más que el tiempo necesario para revertir un número cifrado con una clave pública. En la presente divulgación, la función de troceo puede usarse para transformar el identificador anónimo del sujeto de datos.

Estos cuatro sistemas de criptografía informática - clave simétrica, clave asimétrica, cadena de bloques y función de troceo - pueden combinarse de manera útil en la presente invención. También pueden usarse otras características de cifrado tales como claves de sesión, anillos de claves, claves y testigos temporales, así como cualquier otro sistema de cifrado.

Útil para comprender las realizaciones de la invención es el concepto de consentimiento. El consentimiento es la autorización explícita, específica e informada del sujeto de datos para identificar a las partes que están autorizadas a acceder a los datos personales y datos de interés del sujeto; para autorizar los propósitos para los que se usan los datos y que pueden sobrevivir a la revocación del consentimiento; para identificar las diversas categorías de datos a los que se puede acceder y procesar, dependiendo de la naturaleza y el nivel de autorización consiguiente de las diversas partes de recepción; y para determinar el período de tiempo que los datos pueden almacenarse y procesarse por el ordenador de recepción. El derecho al consentimiento incluye el derecho a revocar el consentimiento, con la consecuencia de que todos los datos personales y todos los datos de interés que se originan con el sujeto de datos deben eliminarse por todos los ordenadores de recepción incluidos en la orden de revocación de consentimiento. Las realizaciones de los sistemas informáticos inventivos descritos en el presente documento emplean este concepto de consentimiento y permiten procedimientos para cambiar el consentimiento.

Una forma de consentimiento incluye una solicitud de transferencia de datos, como se define en el Reglamento General de Protección de Datos de la UE, que permite que un sujeto de datos solicite que sus datos personales almacenados en un servidor informático de controlador de datos se transfieran o copien a otro servidor informático de controlador de datos. En la presente solicitud, es el controlador de datos confiable y su servidor informático los que son los receptores de los datos transferidos bajo una solicitud de transferencia de datos emitida por el sujeto de datos.

Los informes son documentos producidos por el controlador de datos confiable usando datos personales de interés ubicados en su servidor informático y en su base de datos de aplicación, pero de una manera que excluya u oculte el nombre del sujeto de datos o cualquier identificador personal. Los informes usan estadísticas, ciencia de datos y métodos de grandes cantidades de datos. Los informes extraen nuevo conocimiento valioso calculando e infiriendo relaciones entre los elementos obtenidos en los datos personales de interés. Los campos útiles son la publicidad, comercialización y venta de bienes y servicios, finanzas, seguros y medicina, entre otros. En medicina y atención de la salud, los subcampos útiles son el diagnóstico, prescripción inteligente, la clasificación de fármacos y tratamientos en términos de su eficacia, eficacia y seguridad, la identificación de efectos secundarios, reacciones adversas e interacciones farmacológicas, la relación coste/beneficio de los fármacos, dispositivos y tratamientos médicos, todo en términos de atributos del paciente tales como la edad, sexo, características genéticas, gravedad de la enfermedad, la presencia o ausencia de múltiples enfermedades, la administración de múltiples fármacos, cumplimiento de fármacos, adicciones, intolerancias, alergias, vacunas, microbioma y estilo de vida. Los informes también son útiles para identificar cohortes de pacientes que comparten características deseablemente homogéneas o heterogéneas como candidatos para ensayos clínicos.

Los informes usan toda la información disponible en un punto en el tiempo en la base de datos de aplicación del controlador de datos confiable que contiene información de interés de toda la población de sujetos de datos. Cuando los datos personales y la información de interés del sujeto de datos se obtienen mediante consentimiento, las futuras

revocaciones de consentimiento no afectan a los informes, ya que sobreviven a la revocación del consentimiento bajo los términos de consentimiento originales. Esto concluye la descripción de las entidades y funciones útiles en la presente divulgación.

Descripción de la invención. La presente divulgación resuelve los problemas de privacidad intrínsecos a las comunicaciones de Internet a gran escala reemplazando el nombre del sujeto de datos y los identificadores personales en las comunicaciones de datos entre ordenadores con un identificador anónimo, mientras aún permite que el servidor informático de controlador de datos confiable confirme absolutamente la identidad del sujeto de datos anónimo y transmita correctamente datos anónimos de interés al dispositivo informático personal del sujeto de datos propietario. Esto permite que se busquen, recopilen, almacenen y procesen datos personales sensibles sin que el servidor informático de controlador de datos confiable almacene la identidad del nombre del sujeto de datos y, por lo tanto, anula el riesgo de abuso y brecha de la característica de privacidad de muchas comunicaciones basadas en Internet y sistemas informáticos. En el campo de la atención de la salud, esto posibilita el desarrollo de sistemas de historiales médicos electrónicos (EHR) que son intrínsicamente privados.

El sistema y el método descritos requieren un sujeto de datos con un dispositivo informático personal que ejecuta una aplicación de software personal, uno o más proveedores de datos que ejecutan cada uno aplicaciones de software de intercambio de datos en sus servidores informáticos y un controlador de datos confiable que ejecuta una aplicación de software de intercambio de datos en su servidor informático. Los ordenadores de los tres participantes incluyen un módulo de software criptográfico que puede crear claves criptográficas y cifrar y descifrar mensajes. Cada una de las tres aplicaciones de software está configurada para comunicarse de forma segura e intercambiar datos con las otras dos aplicaciones de software. Por comunicación segura se entiende que se emplean medios criptográficos informáticos para garantizar que únicamente tienen lugar comunicaciones autorizadas de la manera descrita en la presente divulgación. De manera útil, el identificador anónimo del sujeto de datos se usará como una clave de cifrado o como parte de un sistema de cifrado en la presente divulgación.

En una realización - la realización general - es útil cualquier medio criptográfico empleado por el módulo de software criptográfico que se ejecuta en los sistemas informáticos de todos los participantes que pueden cifrar de forma segura el identificador anónimo y los datos transmitidos de modo que solo puedan ser descifrados por el sistema informático de recepción legítimo.

En otra realización - la realización de clave asimétrica - los medios criptográficos usan un sistema criptográfico asimétrico de clave pública / clave privada empleado por el módulo de software criptográfico que se ejecuta en los sistemas informáticos de todos los participantes. Estos medios pueden cifrar de forma segura el identificador anónimo y los datos transmitidos de modo que únicamente pueden descifrarse por el sistema informático de recepción pretendido que mantiene y usa las claves apropiadas. Para autenticar las comunicaciones entre el dispositivo informático personal y el servidor informático proveedor de datos o el servidor informático de controlador de datos confiable, el identificador anónimo puede usarse en un procedimiento de firma digital. Una firma digital garantiza que cada ordenador que recibe datos esté seguro de la identidad del ordenador de envío, que no se puede afirmar que el ordenador de envío no originó los datos y que el intercambio de datos es confidencial. Por lo tanto, el identificador anónimo, usado como la clave pública en un sistema de cifrado de clave asimétrica, es también una clave de autenticación y una clave de cifrado. La implementación y el uso de estos métodos son conocidos en la comunidad de criptografía y únicamente se describirán aspectos inventivos destacados en la presente divulgación.

Para hacer que las comunicaciones y el procesamiento sean aún más seguros, una tercera realización añade funcionalidad de función de troceo a la segunda realización, de modo que tanto las claves de función de troceo como las asimétricas se usan para cifrar el identificador anónimo del sujeto de datos y los datos transmitidos.

El dispositivo informático personal del sujeto de datos puede ser, por ejemplo, un teléfono inteligente o una tableta. También se puede usar un ordenador personal o una cuenta personal en un ordenador servidor, pero al ser dispositivos menos personales, son menos adecuados para estas tareas. Concretamente, una cuenta personal en un sistema de servidor puede requerir un nombre de usuario de inicio de sesión definido por el usuario y una contraseña de sistema, que pueden ser datos conocidos por el controlador de datos y, por lo tanto, pueden permitir que los datos personales del sujeto de datos estén asociados con un identificador personal. En ciertos sistemas informáticos, un administrador del sistema puede restablecer una contraseña que permite el acceso inmediato a datos personales e identificables por el administrador. Sin embargo, la invención no se limita a teléfonos inteligentes o tabletas, y es adecuado cualquier dispositivo que se desarrolle en el futuro que tenga suficiente potencia informática y esté al alcance y bajo el control del sujeto de datos.

Para evitar el acceso a las credenciales de inicio de sesión convencionales, tales como nombre de usuario y contraseña, por un controlador de datos o por un administrador de sistemas, por el hecho de que no existen, es una ventaja importante en términos de protección y seguridad de datos personales en la presente solicitud. Para ejecutar el proceso de registro de inicio de sesión del usuario en un servidor central por medio de un identificador anónimo o identificador anónimo cifrado, usando una aplicación de software personal que se ejecuta en el dispositivo informático personal del sujeto de datos, aumenta esa protección y seguridad.

El dispositivo informático personal del sujeto de datos puede configurarse para realizar las etapas descritas en el presente documento por medio de una aplicación de software personal descargada en el dispositivo informático personal desde un sitio web o desde un servicio de distribución de aplicaciones tal como Appstore o Google Play. En todos los casos, la aplicación de software personal se proporciona por el controlador de datos confiable. El propósito de esta aplicación de software personal es recopilar en un único dispositivo informático información personal que pertenece al sujeto de datos que normalmente se distribuye en un número muy grande de servidores informáticos proveedores de datos.

Los sistemas de servidor informático descritos en el presente documento incluyen servidores informáticos operados por los proveedores de datos y por el controlador de datos confiable y, en general, serán sistemas de servidor con una potencia informática, capacidades de almacenamiento y comunicaciones considerables. Los datos se procesan por el proveedor de datos por medio de su aplicación de software de intercambio de datos almacenada en el uno o más servidores informáticos proveedores de datos. Los datos se procesan por el controlador de datos confiable por medio de su aplicación de software de intercambio de datos almacenada en el servidor informático de controlador de datos confiable.

Todos los sistemas informáticos de la presente invención comprenden un procesador, una memoria que puede almacenar instrucciones de programa, subsistemas de comunicaciones, medios de almacenamiento, dispositivos de entrada tales como un teclado, ratón, puntero, pantalla táctil, micrófono o cámara, y dispositivos de salida tales como una pantalla de visualización y un altavoz. Los sistemas informáticos pueden comunicarse entre sí usando redes de telecomunicaciones públicas o privadas, pero se prefiere la red pública y el medio preferido es Internet.

Las operaciones informáticas en la presente divulgación incluyen etapas manuales y etapas automáticas. Las operaciones manuales son aquellas donde se introducen datos por un sujeto de datos configurando la aplicación de software personal en su dispositivo informático personal. Durante la instalación de la aplicación de software personal, el sujeto de datos introduce los datos de identificación personal mediante los que el servidor informático proveedor de datos podrá identificar los datos de salud del sujeto de datos. Esto puede ser el nombre o identificadores personales, o ambos. Opcionalmente, el sujeto de datos también introduce una declaración de consentimiento y una solicitud de transferencia de datos, así como cualquier otra indicación necesaria para establecer preferencias de usuario o datos requeridos para la operación de programa posterior y que variará dependiendo de los requisitos funcionales específicos de las aplicaciones de software. Otras tareas manuales por el sujeto de datos incluyen la selección de opciones de menú en la aplicación de software personal durante el uso.

Todas las demás tareas descritas en el presente documento son tareas automáticas y se producen automáticamente bajo el control de un programa informático para gestionar todo el procesamiento de datos en el dispositivo informático personal del sujeto de datos y en los servidores informáticos del uno o más proveedores de datos y del controlador de datos confiable y las comunicaciones e intercambios de datos entre ellos.

La presente invención se refiere a habilitar una secuencia de solicitudes, recuperación, almacenamiento, procesamiento e intercambio de datos bajo el control de programas informáticos ejecutados en los datos personales del sujeto de datos en su dispositivo informático personal, en el uno o más servidores informáticos proveedores de datos que buscan, anonimizan y transmiten datos de interés anonimizados relacionados con el sujeto de datos, y en el servidor informático de controlador de datos confiable que recibe, almacena y acumula los datos de interés anonimizados y los devuelve al dispositivo informático personal del sujeto de datos anónimo.

El servidor informático de controlador de datos confiable no almacena ninguna información sobre o perteneciente al nombre o identificadores personales del sujeto de datos, ni ninguna información de dirección electrónica, tal como el número de teléfono celular, dirección electrónica o dirección de internet del dispositivo informático personal del sujeto de datos. No almacenar estos datos es una forma eficiente de evitar que los ordenadores vulneren accidental, negligente o maliciosamente los datos personales del sujeto de datos y los derechos de privacidad asociados. Por lo tanto, elementos de datos que identifican al sujeto de datos, tales como el nombre o los identificadores personales no deben comunicarse al servidor informático de controlador de datos confiable, ni proporcionarse medios al servidor informático de controlador de datos confiable para identificar al sujeto de datos por nombre, identificadores personales, nombre de usuario de inicio de sesión o contraseña de sistema. En consecuencia, los ordenadores de la presente invención no están configurados para identificar sujetos de datos usando un nombre de usuario de inicio de sesión convencional y contraseñas de sistema. Una contraseña de sistema es un código confidencial normalmente elegido por el sujeto de datos que se almacena en el sistema informático de cualquier controlador de datos que gestiona la cuenta de usuario de ordenador del sujeto de datos.

En su lugar, la aplicación de software personal en el dispositivo informático personal usa un número único para identificar al sujeto de datos - el identificador anónimo. El número es de tal dimensión que la probabilidad de que al menos dos seres humanos compartan el mismo identificador anónimo y diferentes ordenadores almacenen y usen el mismo identificador anónimo para identificar a más de un ser humano se considera cercana a cero. El identificador anónimo es, por lo tanto, también una clave de identificación del sujeto de datos.

Hay al menos dos formas en que un sistema informático puede generar el identificador anónimo, empleando ambas

el módulo de software criptográfico que se ejecuta en el dispositivo informático personal. La primera es generando un único número aleatorio complejo y se usará en comunicaciones criptográficas entre todos los sistemas informáticos. Usarán el identificador anónimo del sujeto de datos también como la clave criptográfica en un sistema criptográfico de clave simétrica. La segunda forma es usar sistemas criptográficos de clave de cifrado asimétrica. En una primera etapa, el módulo de software criptográfico genera un número aleatorio, que será la clave criptográfica privada del sujeto de datos. A partir de la clave privada, el módulo de software criptográfico deriva matemáticamente la clave criptográfica pública, usando, por ejemplo, el método publicado del algoritmo de firma digital de curva elíptica. Esto puede usarse para comunicaciones cifradas entre los sistemas informáticos del sujeto de datos, el uno o más proveedores de datos y el controlador de datos confiable.

La clave criptográfica pública del sujeto de datos también será su identificador anónimo, pero su uso será diferente de la convención, ya que seguirá siendo confidencial y únicamente conocido por los ordenadores del sujeto de datos y del controlador de datos confiable. Dado que el identificador anónimo puede ser una clave de identificación, una clave de autenticación y una clave de cifrado, debe estar severamente protegido, a través de cifrado, generando el identificador anónimo cifrado.

Para mayor seguridad, al identificador anónimo original del sujeto de datos puede aplicarse una función de troceo por el módulo de software criptográfico del sujeto de datos en el dispositivo informático personal, de modo que pueda transmitirse a proveedores de datos de una manera que oculte el identificador anónimo original. En esta realización, cuando el sujeto de datos instala la aplicación de software personal en su dispositivo informático personal, el proceso de instalación está configurado para enviar el identificador anónimo original al servidor informático de controlador confiable. Al recibirlo, el servidor informático de controlador de datos confiable aplica el algoritmo de función de troceo al identificador anónimo original y obtiene el identificador anónimo con función de troceo, que lo almacena en el registro de entrada del sujeto de datos en su base de datos de registro de usuario. En transmisiones posteriores de información de interés perteneciente al sujeto de datos, entre el servidor informático proveedor de datos y el servidor informático de controlador de datos confiable, los datos del sujeto se identifican por el primero mediante el identificador anónimo con función de troceo del sujeto. Al recibirlo, el servidor informático de controlador de datos confiable busca en su base de datos de registro de datos ese identificador anónimo con función de troceo y, al encontrar una coincidencia, lee el identificador anónimo original del sujeto de datos en el mismo registro y almacena los datos de interés recibidos bajo la identidad de ese identificador anónimo.

En todas las realizaciones criptográficas, es deseable que el identificador anónimo cifrado únicamente se descifre por el servidor informático de controlador de datos confiable. Por lo tanto, el identificador anónimo cifrado y las claves criptográficas necesarias para descifrarlo únicamente se conocerán por los módulos de software criptográfico que se ejecutan en el dispositivo informático personal del sujeto de datos y en el servidor informático de controlador de datos confiable y serán secretos para todos los demás ordenadores, tales como los servidores informáticos proveedores de datos.

Dada la existencia de numerosos métodos de cifrado y transformación de datos y para simplificar la presente divulgación, las expresiones "cifrar", "función de troceo", "identificador anónimo cifrado", "datos cifrados", "firmado digitalmente" (y sus contrapartes "descifrar", "identificador anónimo descifrado", "datos descifrados", "firma digital verificada") se usará ahora sin referencia continua al método de cifrado o transformación de datos usado, usando únicamente las palabras "cifrado" y "descifrado" excepto cuando el contexto así lo requiera. No obstante, una persona con una habilidad razonable en criptografía podrá identificar el método más apropiado para cada uso.

La presente divulgación describirá ahora la operación del presente sistema y método para manejar datos personales anonimizados. Este sistema y método se usan para buscar y obtener datos personales identificados relacionados con un sujeto de datos, que comprende la descarga e instalación de una aplicación de software personal en un dispositivo informático personal y el sujeto de datos que introduce el al menos nombre o identificadores personales o ambos y el consentimiento opcional, la solicitud de transferencia de datos y las preferencias de usuario. El módulo de software criptográfico también se descarga e instala y genera un identificador anónimo para el sujeto de datos, así como una versión cifrada, el identificador anónimo cifrado. La aplicación de software personal envía los datos y el identificador anónimo cifrado al uno o más servidores informáticos proveedores de datos, que buscan y obtienen la información de interés del sujeto de datos almacenada en su una o más bases de datos de aplicación, eliminan todos los identificadores personales para desidentificar y anonimizar la información y el sujeto de datos, transmiten la información anonimizada y el identificador anónimo cifrado a un servidor informático de controlador de datos confiable, que descifra y valida el identificador anónimo del sujeto de datos y almacena, procesa y posteriormente devuelve los datos anonimizados al dispositivo informático personal del sujeto de datos anónimo.

En más detalle, justo después de la instalación, la aplicación de software personal en el dispositivo informático personal contacta con todos los servidores informáticos proveedores de datos participantes que probablemente tengan datos personales relacionados con el sujeto de datos. Los servidores informáticos proveedores de datos ejecutan una aplicación de software de intercambio de datos configurada para comunicarse de forma segura con la aplicación de software personal. Un servidor informático proveedor de datos recibe los datos de la aplicación de software personal, incluyendo el al menos nombre o identificadores personales o ambos y el consentimiento opcional, la solicitud de transferencia de datos, preferencias de usuario e identificador anónimo cifrado, y por medio de los identificadores

personales, busca en sus bases de datos de aplicación datos personales de interés que pertenecen al sujeto de datos y obtiene datos identificados. Al encontrarlos, la aplicación de software de intercambio de datos elimina cualquiera y todos los identificadores personales de los datos de interés identificados: nombre, fecha de nacimiento completa, dirección, números de identificación personal, número de teléfono celular, dirección de correo electrónico, dirección de internet y similares, para desidentificar y anonimizar los datos de interés del sujeto de datos. Estas acciones se llevan a cabo por todos los servidores informáticos proveedores de datos contactados por la aplicación de software personal del sujeto de datos.

La aplicación de software de intercambio de datos en cada servidor informático proveedor de datos añade a continuación a los datos de interés anonimizados el identificador anónimo cifrado del sujeto de datos y la información opcional y los transmite a la aplicación de software de intercambio de datos en el servidor informático de controlador de datos confiable.

El servidor informático de controlador de datos confiable recibe la transmisión de datos y verifica si se refiere a un sujeto de datos nuevo o existente. Esto se hace descifrando la aplicación de software de intercambio de datos el identificador anónimo cifrado del sujeto de datos, y buscando el identificador anónimo descifrado del sujeto de datos en la base de datos de registro de usuario del servidor informático de controlador de datos confiable.

Si no lo encuentra, el sujeto de datos es nuevo y la aplicación de software de intercambio de datos abre una nueva entrada para el sujeto de datos registrando su identificador anónimo, el consentimiento opcional, solicitud de transferencia de datos y preferencias en la base de datos de registro de usuario y los metadatos de transmisión (por ejemplo, indicación de tiempo de la comunicación, identidad y dirección del proveedor de datos de origen, etc.) en el archivo de registro de transmisiones, del servidor informático de controlador de datos confiable. Si lo encuentra, el sujeto de datos es, por lo tanto, uno existente y la aplicación de software de intercambio de datos registra los metadatos de transmisión en el archivo de registro de transmisiones en el servidor informático de controlador de datos confiable. Posteriormente y en ambos casos, la aplicación de software de intercambio de datos registra el identificador anónimo y los datos de interés anonimizados en las bases de datos de aplicación del servidor informático de controlador de datos confiable.

La transmisión de datos anonimizados desde el servidor informático proveedor de datos al servidor informático de controlador de datos confiable se producirá periódicamente, cada vez que se introducen nuevos datos personales que pertenecen al sujeto de datos en las bases de datos de aplicación del uno o más servidores informáticos proveedores de datos participantes. La aplicación de software de intercambio de datos en el servidor informático proveedor de datos se configurará para identificar los nuevos datos para su posterior transmisión al servidor informático de controlador de datos confiable. Esta transmisión periódica se producirá siempre que el sujeto de datos no revoque su consentimiento para el acceso y procesamiento de datos personales, a través de su aplicación de software personal, una revocación que se difundirá a todos los servidores que participan en el presente sistema informático y de intercambio de datos. Con el paso del tiempo, el servidor informático proveedor de datos continuará transmitiendo nuevos datos y el servidor informático de controlador de datos confiable acumulará una cantidad sustancial de datos de interés anonimizados, identificados únicamente por el identificador anónimo del sujeto de datos.

A continuación, se describirá el método mediante el que el servidor informático de controlador de datos confiable devuelve datos de interés anonimizados a la aplicación de software personal de un sujeto de datos anónimo. La aplicación de software personal en el dispositivo informático personal y la aplicación de software de intercambio de datos del servidor informático de controlador de datos confiable establecen comunicación a través de la red de comunicaciones y la aplicación de software de intercambio de datos transmite los datos de interés anonimizados a la aplicación de software personal devolviendo de esta manera los datos personales e información de interés para el dispositivo informático personal del sujeto de datos anónimo.

Esto se logra por medio de una sesión de comunicaciones que siempre se inicia por la aplicación de software personal en el dispositivo informático personal del sujeto de datos, que se conecta a la dirección electrónica conocida del servidor informático de controlador de datos confiable. La aplicación de software de intercambio de datos en el servidor informático de controlador de datos confiable debe esperar a que la aplicación de software personal inicie la sesión de comunicaciones, impidiendo que el servidor informático de controlador de datos confiable inicie una sesión de comunicación de este tipo, ya que no tiene ningún elemento de contacto, números o direcciones.

Las comunicaciones seguras entre el dispositivo informático personal de sujeto de datos y el servidor informático de controlador de datos confiable se logran transmitiendo la aplicación de software personal una solicitud de intercambio de datos al servidor informático de controlador de datos confiable, que puede validarse de dos maneras diferentes. La aplicación de software personal y el módulo de software criptográfico pueden enviar la solicitud y el identificador anónimo del sujeto de datos en un formato firmado digitalmente, donde el identificador anónimo está cifrado con la clave privada del módulo de software criptográfico, al que se adjunta la clave pública del sujeto de datos. El módulo de software criptográfico en el servidor informático de controlador de datos confiable descifra el mensaje usando la clave pública que se adjuntó al mensaje. Si el contenido del mensaje descifrado es el mismo que la clave pública usada para descifrarlo, a continuación, se valida la firma digital y el mensaje.

En un segundo método, una solicitud identificada exclusivamente por el identificador anónimo del sujeto de datos puede validarse por la aplicación de software de intercambio de datos en el servidor informático de controlador de datos confiable, que la recibe y la compara con entradas similares en la base de datos de registro de usuario en el servidor informático de controlador de datos confiable. Si se encuentra una coincidencia, esta es una confirmación de que se ha recibido una solicitud válida y que el identificador anónimo almacenado y el identificador anónimo recibido corresponden al mismo sujeto de datos anónimo.

Siguiendo cualquiera de estos dos métodos de verificación, la aplicación de software de intercambio de datos en el servidor informático de controlador de datos confiable está segura de devolver los datos de interés anonimizados al dispositivo informático personal de su sujeto de datos propietario legítimo. Este método y sistema proporciona a los ordenadores de la presente invención un nivel de seguridad operativa con respecto a los derechos de privacidad que hasta ahora estaba ausente o era deficiente en las comunicaciones basadas en Internet y los sistemas informáticos.

Seleccionar el sistema criptográfico de clave asimétrica para generar el identificador anónimo y proporcionar pares de claves criptográficas asimétricas a todos los ordenadores de la presente invención - del sujeto de datos, de proveedores de datos y del controlador de datos confiable - así como el uso de una función de troceo para transformar el identificador anónimo original satisface con mayor eficiencia y seguridad las deficiencias actuales en los sistemas informáticos existentes con respecto al riesgo de abuso de privacidad relacionado con datos personales.

De esta manera, cuando la aplicación de software personal contacta por primera vez con el uno o más servidores informáticos proveedores de datos y transmite los datos del sujeto introducidos durante la instalación de la aplicación de software personal en el dispositivo informático personal del sujeto de datos, el identificador anónimo original del sujeto de datos se le aplicará función de troceo o cifrará y, por lo tanto, seguirá sirviendo como un identificador único para el sujeto de datos, pero sin revelar el identificador anónimo original. En consecuencia, el servidor informático proveedor de datos no puede asociar el nombre y los identificadores personales del sujeto de datos, que se almacenan en y son conocidos por ese servidor informático proveedor de datos, con el identificador anónimo original del sujeto de datos. Esto garantiza la confidencialidad de la clave pública del sujeto de datos, que también es su identificador anónimo. Cuando el servidor informático proveedor de datos transmite los datos de interés anonimizados y el identificador anónimo cifrado al servidor informático de controlador de datos confiable, el servidor informático de controlador de datos confiable usa su clave criptográfica privada para descifrar el identificador anónimo original del sujeto de datos. De esta manera, será imposible para cualquier parte usar un ordenador o para cualquier ordenador, excepto el sujeto de datos y el controlador de datos confiable y sus respectivos ordenadores, para conocer el identificador anónimo del sujeto de datos y usarlo para recuperar ilegal o maliciosamente los datos de interés del sujeto de datos del servidor informático de controlador de datos confiable, y, a continuación, usar los datos en la vulneración de los derechos de privacidad del sujeto de datos. Incluso si el ordenador que intercepta puede recopilar una cantidad considerable de información de interés, en ausencia del nombre o identificadores personales del sujeto de datos, no es identificable o relacionable con una persona conocida.

Cuando la aplicación de software personal en el dispositivo informático personal y la aplicación de software de intercambio de datos en el servidor informático de controlador de datos confiable comunican y transmiten datos, la sesión de comunicaciones se inicia en la mayoría de los casos automáticamente, de acuerdo con las preferencias predeterminadas existentes en la aplicación de software personal, periodos normalmente diarios, semanales o mensuales, o incluso más largos. Esta frecuencia depende de la naturaleza de los datos. En el caso de la atención de la salud, un valor predeterminado adecuado es mensual, pero, si una persona está hospitalizada, un intervalo más apropiado es una actualización diaria. Por esta razón, el sujeto de datos puede cambiar la frecuencia de actualización en su aplicación de software personal a un intervalo deseado o incluso seleccionar un botón de opción de actualización inmediata en la aplicación de software personal.

Para actualizaciones programadas, la frecuencia se comunicará por la aplicación de software personal a la aplicación de software de intercambio de datos en el uno o más servidores informáticos proveedores de datos. Para una actualización inmediata, la solicitud irá directamente al software de intercambio de datos en el servidor informático de controlador de datos confiable, para la recuperación de datos de interés adquiridos recientemente.

En todas las realizaciones, durante la comunicación de mensajes que contienen datos de interés anonimizados desde el uno o más servidores informáticos proveedores de datos al servidor informático de controlador de datos confiable, y el registro de un nuevo sujeto de datos anónimo en la base de datos de registro de usuario del controlador de datos confiable, y la comunicación de datos de interés anonimizados desde el servidor informático de controlador de datos confiable al dispositivo informático personal del sujeto de datos anónimo, el sujeto de datos nunca usa y la aplicación de software personal nunca requiere que use un nombre de usuario definido por el usuario convencional y una contraseña de sistema, que identificaría indeseablemente al sujeto de datos. El acceso a la aplicación de software personal puede asegurarse mediante el uso de una contraseña de bloqueo de pantalla local, almacenarse exclusivamente en el dispositivo informático personal, o por medios biométricos tales como una huella digital o reconocimiento facial presente localmente en dispositivos informáticos personales. La verificación de identidad es únicamente y siempre por medio del identificador anónimo.

Existen varias aplicaciones de software para recopilar los datos personales de un sujeto de datos y este es el caso en

aplicaciones de registro de atención de la salud y de salud electrónicas. Sin embargo, tales aplicaciones normalmente están asociadas con un proveedor de atención de la salud o una compañía de seguros y no cubren todos los proveedores de datos donde pueden almacenarse los registros de un sujeto de datos. La presente solicitud divulga un método y un sistema donde los datos personales pueden recopilarse universalmente, desde donde sea que pueda almacenarse en una multiplicidad de servidores informáticos proveedores de datos participantes y, a continuación, reenviarse en forma anonimizada y devolverse en una forma organizada fácil de entender al dispositivo informático personal del sujeto de datos.

Devolver la información de interés del sujeto de datos en una sesión de comunicaciones siempre iniciada por la aplicación de software personal del sujeto de datos e identificada por el identificador anónimo resuelve la paradoja de reversibilidad / irreversibilidad de anonimización y permite que el servidor informático de controlador de datos confiable se comunique de forma segura con el dispositivo informático personal de sujeto de datos y para transmitir información personal valiosa y conocimiento científico derivado del procesamiento a gran escala de datos personales, sin conocer el nombre del sujeto de datos, número de teléfono celular, dirección de correo electrónico o dirección de dispositivo informático personal.

En una realización de la invención, un padre puede almacenar la información de interés de un niño en el dispositivo informático personal del padre y, a continuación, permitir que la información del niño se elimine del dispositivo del padre y se transfiera al dispositivo del niño, por ejemplo, al alcanzar una cierta edad legal.

En otra realización de la invención aplicable a la atención de la salud, el sujeto de datos puede, por medio de la aplicación de software personal, designar a un profesional de la atención de la salud que estará autorizado a recibir los registros médicos del sujeto de datos. Para conseguir esto, el sujeto de datos hace que la aplicación de software personal envíe el identificador anónimo del sujeto de datos y el nombre del profesional de la atención de la salud a la aplicación de software de intercambio de datos en el servidor informático de controlador de datos confiable. El profesional de atención de la salud ejecutará una aplicación en su ordenador que está conectado a través de una red de comunicaciones a la misma aplicación de software de intercambio de datos. Esta aplicación en el servidor informático de controlador de datos confiable recibirá la solicitud del sujeto de datos y el identificador anónimo y el nombre del profesional de atención de la salud. A continuación, recuperará los registros médicos del sujeto de datos de su base de datos de aplicación y los enviará al ordenador conectado a la aplicación de software de intercambio de datos de salud cuya identidad de usuario coincide con el nombre del profesional de atención de la salud designado por el sujeto de datos. Por lo tanto, los registros de atención de la salud pueden compartirse por el sujeto de datos con el profesional de atención de la salud elegido, y la compartición de datos se produce sin que el servidor informático de controlador de datos confiable conozca el nombre del sujeto de datos.

En otra realización, la aplicación de software personal está configurada para detectar la presencia de la misma aplicación de software personal instalada en otros dispositivos informáticos personales de otros sujetos de datos que están cerca, y, a través de wifi o Bluetooth, las aplicaciones de software personal difunden, reciben y almacenan los identificadores anónimos cifrados de los demás. Esta realización es particularmente útil en situaciones epidémicas, cuando sea necesario conocer la identificación, preferentemente anónima, de todos los que estaban cerca de una persona infectada, para contactar con todos los interesados y enviarles consejos relevantes a sus aplicaciones de software personales.

Otra realización implica que, la aplicación de software personal, durante su instalación, contacte en primer lugar con un servidor informático de verificación de identidad conocido, para el propósito de garantizar absolutamente que el sujeto de datos es de hecho la persona indicada por su nombre, y no otra persona que intenta hacerse pasar por el sujeto de datos para obtener ilegalmente la información personal de interés del sujeto de datos. Únicamente tras la verificación de identidad, como se describe, por ejemplo, en la solicitud de patente PT 115.304, se permitirá que la aplicación de software personal concluya con éxito su instalación en el dispositivo informático personal, mediante un mensaje de servidor informático de verificación de identidad que lo permita. El servidor informático de verificación de identidad también puede almacenar la lista de servidores informáticos proveedores de datos que probablemente almacenen información de interés del sujeto de datos. En este caso, el servidor informático de verificación de identidad puede programarse para garantizar la distribución de los datos de registro de usuario del sujeto de datos a todos los servidores informáticos proveedores de datos participantes. Esto libera al dispositivo informático personal de estar atado a un proceso de registro de sujeto de datos que puede ser largo. Esta posible función para el servidor informático de verificación de identidad no altera sustancialmente la presente divulgación, ya que después de verificar la identidad del sujeto de datos, transmite datos a los servidores informáticos proveedores de datos exactamente de la misma manera que se describe en el presente documento con respecto a los intercambios y transmisiones de datos entre el dispositivo informático personal y el uno o más servidores informáticos proveedores de datos. Los medios para controlar el intercambio seguro de datos en esta realización pueden incluir claves de cifrado asimétricas, firmas digitales, funciones de troceo y cadena de bloques.

Otra realización implica la posibilidad de recuperar la información de interés de un sujeto de datos, en caso de pérdida, destrucción, robo, reinstalación o mejora del dispositivo informático personal del sujeto de datos. En este punto, se puede usar un nuevo dispositivo informático personal, descargarse e instalarse de nuevo la aplicación de software personal, generándose un nuevo identificador anónimo y recuperarse la cuenta de usuario del ordenador del sujeto

de datos, reiniciar el proceso de flujo de datos a través del uno o más servidores informáticos proveedores de datos y permitir que la información de interés previamente existente almacenada en el servidor informático de controlador de datos confiable se vuelva a asociar con el nuevo identificador anónimo de sujeto de datos, sin transmitir o revelar la identidad de nombre o los identificadores personales del sujeto de datos al servidor informático de controlador de datos confiable. Los medios para esta recuperación incluyen un ordenador que almacena antes del proceso de recuperación al menos el nombre del sujeto de datos, identificadores personales y el identificador anónimo cifrado original. Por lo tanto, los servidores informáticos proveedores de datos y los servidores informáticos de verificación de identidad pueden ser útiles en esta recuperación.

Descripción de sumario de los dibujos

La figura 1a es un diagrama de bloques de una arquitectura de sistema usada para descargar e instalar una aplicación de software personal en un dispositivo informático personal, de acuerdo con una realización ilustrativa de la presente divulgación.

La figura 1b es un diagrama de bloques de una arquitectura de sistema informático usada para conectar un dispositivo informático personal, un servidor informático proveedor de datos, un servidor informático de controlador de datos confiable y para establecer comunicaciones entre todos ellos, de acuerdo con una realización ilustrativa de la presente divulgación.

La figura 2 es un diagrama de bloques de un dispositivo informático personal, de acuerdo con una realización ilustrativa de la presente divulgación.

La figura 3 es un diagrama de bloques de un servidor informático proveedor de datos, de acuerdo con una realización ilustrativa de la presente divulgación.

La figura 4 es un diagrama de bloques de un servidor informático de controlador de datos confiable, de acuerdo con una realización ilustrativa de la presente divulgación.

La figura 5 es un diagrama de flujo del flujo de programa que empieza con la instalación de la aplicación de software personal en el dispositivo informático personal y finaliza con la transferencia de la información de interés al servidor informático de controlador de datos confiable, de acuerdo con una realización ilustrativa de la presente divulgación.

La figura 6 es un diagrama de flujo del flujo de programa que empieza con la transmisión de solicitud de intercambio de datos por la aplicación de software personal y finaliza con el acceso y uso del sujeto de datos de la información de interés personal en su dispositivo informático personal, de acuerdo con una realización ilustrativa de la presente divulgación.

En los dibujos, números similares hacen referencia a elementos y características similares en la descripción.

Descripción detallada de los dibujos

En la figura 1a, el sujeto de datos conecta su dispositivo informático personal a la red de comunicaciones digitales móvil pública, tal como el sistema GSM, por ejemplo, o Internet, o cualquier otra red de comunicaciones - colectivamente la red de comunicaciones. A continuación, el sujeto de datos descarga e instala una aplicación de software personal 100 y un módulo de software criptográfico 101 en su dispositivo informático personal 110. La aplicación de software personal 100 y el módulo de software criptográfico 101 se descargan desde un sistema de distribución de software apropiado 105, tal como AppStore o Google Play, o un sitio web de Internet, al que el sujeto de datos se conecta usando su dispositivo informático personal 110. El sujeto de datos tiene conocimiento de la aplicación de software personal 100 a través del boca a boca, redes sociales o un anuncio convencional, que lo identifican como una aplicación de software personal publicada por un controlador de datos confiable para recopilar de forma segura datos personales que pertenecen al sujeto de datos.

En la figura 1b, una vez que se ha producido la descarga, tiene lugar la instalación de la aplicación de software personal 100 y el sujeto de datos introduce al menos su nombre y puede introducir otros identificadores personales y términos de consentimiento. La aplicación de software personal 100 genera un identificador anónimo, así como su versión cifrada usando la clave pública conocida del controlador de datos confiable.

La aplicación de software personal 100 del dispositivo informático personal 110 envía el mensaje de datos completo - datos introducidos por el sujeto de datos y el identificador anónimo cifrado - al uno o más servidores informáticos proveedores de datos 120, conocidos por la aplicación de software personal, que es probable que contenga datos personales relacionados con el sujeto de datos. El uno o más servidores informáticos proveedores de datos 120 comprenden una aplicación de software de intercambio de datos 125, configurada para intercambiar datos de forma segura con la aplicación de software personal 100 y almacenarlos.

La aplicación de software de intercambio de datos 125 busca las bases de datos de aplicación del servidor informático

proveedor de datos 120 y extrae la información de interés relacionada con el sujeto de datos. La aplicación de software de intercambio de datos 125 anonimiza la información de interés eliminando el nombre y los identificadores personales y reemplazándolos con el identificador anónimo cifrado del sujeto de datos y la transmite al servidor informático de controlador de datos confiable 130. Este servidor 130 también comprende una aplicación de software de intercambio de datos 135 configurada para intercambiar datos de forma segura con la aplicación de software de intercambio de datos 125 en el uno o más servidores informáticos proveedores de datos 120. Esta extracción, anonimización y transmisión de datos se produce a continuación periódicamente bajo el control de la aplicación de software de intercambio de datos 125 que se ejecuta en el uno o más servidores informáticos proveedores de datos 120.

La aplicación de software de intercambio de datos 135 en el servidor informático de controlador de datos confiable 130 recibe el mensaje de datos desde la aplicación de software de intercambio de datos 125 en el servidor informático proveedor de datos 120, incluyendo la información de interés anonimizada y el identificador anónimo cifrado.

La aplicación de software de intercambio de datos 135 descifra o valida el identificador anónimo del sujeto de datos y almacena la información de interés anonimizada. A intervalos regulares, la aplicación de software de intercambio de datos 135 del servidor informático de controlador de datos confiable 130 transmite la información de interés recién recibida a la aplicación de software personal 100 en el dispositivo informático personal 110 del sujeto de datos que está identificado por el mismo identificador anónimo que la información de interés anonimizada.

En la figura 2, el dispositivo informático personal 110 se ilustra en términos de sus componentes de hardware y software esenciales. El dispositivo informático personal 110 comprende un procesador principal 200, un subsistema de comunicaciones 210 diseñado para comunicarse a través de la red de comunicaciones con todos los servidores informáticos proveedores de datos 120 y el servidor informático de controlador de datos confiable 130, un dispositivo de entrada 220, una pantalla 230 y un subsistema de medios de almacenamiento 235 que almacenan programas informáticos y datos. El procesador 200 interactúa con la memoria 240 que contiene programas informáticos y datos recuperados del subsistema de almacenamiento de medios 235. El procesador 200 carga en la memoria 240, según sea necesario, las instrucciones de programa 250, la aplicación de software personal 100, el módulo de software criptográfico 101 y datos de archivos y bases de datos de aplicaciones que almacenan la información de interés 280 recibida desde el servidor informático controlador de datos confiable 130.

La figura 3 ilustra los componentes de hardware y software esenciales del uno o más servidores informáticos proveedores de datos.

El uno o más servidores informáticos proveedores de datos 120 comprenden un procesador principal 300, un subsistema de comunicaciones 310 diseñado para comunicarse a través de la red de comunicaciones con todos los dispositivos informáticos personales de sujeto de datos 110 y el servidor informático de controlador de datos confiable 130, un dispositivo de entrada 320, una pantalla 330 y un subsistema de medios de almacenamiento 335 que almacenan programas informáticos y datos. El procesador 300 interactúa con la memoria 340 que contiene programas informáticos y datos recuperados del subsistema de almacenamiento de medios 335. El procesador 300 carga en la memoria 340, según sea necesario, instrucciones de programa 350, la aplicación de software de intercambio de datos 125, el módulo de software criptográfico 301, la base de datos de registro de usuario 370, conteniendo la base de datos de aplicación 380 los datos personales identificados del sujeto de datos y los archivos de registro de transacción 390 que contienen los metadatos de comunicaciones de todas las sesiones de intercambio de datos que comprenden al menos la identidad del ordenador de origen y la indicación de tiempo del evento de intercambio de datos.

La figura 4 ilustra los componentes de hardware y software esenciales del servidor informático de controlador de datos confiable.

El servidor informático de controlador de datos confiable 130 comprende un procesador principal 400, un subsistema de comunicaciones 410 diseñado para comunicarse a través de la red de comunicaciones con el dispositivo informático personal de sujeto de datos 110 y los servidores informáticos proveedores de datos 120, un dispositivo de entrada 420, una pantalla 430 y un subsistema de medios de almacenamiento 435 que almacenan programas informáticos y datos. El procesador 400 interactúa con la memoria 440 que contiene programas informáticos y datos recuperados del subsistema de almacenamiento de medios 435, El procesador 400 carga en la memoria 440, según sea necesario, instrucciones de programa 450, la aplicación de software de intercambio de datos 135, el módulo de software criptográfico 401, la base de datos de registro de usuario 470, la base de datos de aplicación 480 que contiene la información anonimizada de interés del sujeto de datos, los archivos de registro de transacción 490 que contienen los metadatos de comunicaciones de todas las sesiones de intercambio de datos que comprenden al menos la identidad del ordenador de origen y la indicación de tiempo del evento de intercambio de datos y la aplicación de software de ciencia de datos 495. En uso, es esta aplicación de software de ciencia de datos la que procesará la información de interés anonimizada almacenada a una escala muy grande en la base de datos de aplicación 480 para producir los informes descritos anteriormente de los que se derivará nueva información y nuevo conocimiento. Estos informes tendrán un valor económico significativo y, en ciertos campos, tales como la atención de la salud, un interés público considerable.

La operación de los sistemas informáticos de las figuras 1a, 1b, 2, 3 y 4 se explicará ahora en detalle a través de los

diagramas de flujo en las figuras 5 y 6. Las etapas de programa están numeradas por números que pertenecen a las series 500 y 600, pero también se hace referencia a elementos de las figuras anteriores.

La figura 5 ilustra el proceso mediante el que un sujeto de datos se registra en el sistema informático de la presente divulgación, y cómo se recopilan datos de interés desde el uno o más servidores informáticos proveedores de datos 120 y se transmiten al servidor informático de controlador de datos confiable 130. En la etapa 500, el sujeto de datos descarga la aplicación de software personal 100 y el módulo de software criptográfico asociado 101 desde un servicio de distribución de aplicaciones adecuado o un sitio web 105, en su dispositivo informático personal 110. Durante el proceso de instalación, el sujeto de datos introduce datos de identificación personal a través de un dispositivo de entrada 220 en la aplicación de software personal 100, tal como nombre, sexo, fecha de nacimiento, dirección, código postal e identificadores personales, tal como el número de tarjeta de ID de un ciudadano, número de permiso de conducción, número de seguridad social o número de identificación fiscal - tantos como puedan existir, y esto ayudará en la recuperación posterior de datos personales en los servidores informáticos proveedores de datos.

Cuando las leyes para proteger los datos personales así lo requieran, el sujeto de datos indica a través del dispositivo de entrada de datos 220 en la aplicación de software personal 100 su consentimiento para la recuperación de sus datos personales, desde cualquier servidor informático proveedor de datos 120 en el que puedan almacenarse, y transferirlos a y ser procesados por el servidor informático de controlador de datos confiable 130. Típicamente, la aplicación de software personal 100 habrá sido desarrollada y emitida por un controlador de datos confiable específico, y se configurará para mostrar el nombre de ese controlador de datos confiable en la pantalla del dispositivo informático personal 110, de modo que el sujeto de datos tenga completamente claro a qué sistema informático se transferirán o copiarán sus datos personales anonimizados. El sujeto de datos también puede introducir cualquier dato de preferencia u opción solicitado por la aplicación de software personal 100 usando el dispositivo de entrada 220.

Una vez concluida la etapa de entrada de datos, en la etapa 510, un módulo de software criptográfico 101 en el dispositivo informático personal 110 genera un identificador anónimo y una versión cifrada del mismo. El identificador anónimo puede generarse usando un sistema de claves simétricas o un sistema de claves asimétricas, dependiendo de la realización y el nivel de seguridad deseado, pero, independientemente del sistema adoptado para generarlo, el identificador anónimo y el identificador anónimo cifrado siempre se asociarán al sujeto de datos de origen e identificarán como una clave de identificación todos los datos personales recuperados posteriormente en el uno o más servidores informáticos proveedores de datos 120 y transmitidos al servidor informático de controlador de datos confiable 130.

En la realización general, cuando se usa una clave criptográfica simétrica, el identificador anónimo puede generarse para cumplir la función de una clave de cifrado, usando la norma de cifrado avanzado comprendida en el módulo de software criptográfico 101 del dispositivo informático personal 110.

En la realización de clave asimétrica, las claves criptográficas asimétricas se generan usando el sistema preferido del algoritmo de firma digital de curva elíptica. La clave privada se generará aleatoriamente por el módulo de software criptográfico 101 en el dispositivo informático personal 110 y a partir de esta clave privada el módulo de software criptográfico 101 derivará matemáticamente una clave criptográfica pública. Esta clave pública también será el identificador anónimo del sujeto de datos. A continuación, el módulo de software criptográfico 101 selecciona la clave pública / identificador anónimo generado y produce una versión cifrada usando la clave criptográfica pública conocida del servidor informático controlador de datos confiable 130, o usando cualquiera de los otros métodos criptográficos o de transformación descritos en la presente divulgación. La clave pública del servidor informático de controlador de datos confiable 130 se conoce públicamente, y se almacena en el módulo de software criptográfico 101 en el dispositivo informático personal 110. Esto significa que, si la clave pública cifrada del sujeto de datos se transmite o se intercepta por otros ordenadores que no tienen los medios para descifrar el identificador anónimo cifrado, nunca conocerán el identificador anónimo original del sujeto de datos. Por lo tanto, cuando se transmite al uno o más servidores informáticos proveedores de datos 120 como parte del proceso de registro inicial descrito en esta figura 5, se impide que los servidores informáticos proveedores de datos 120 conozcan el identificador anónimo de texto sin formato del sujeto de datos y, por lo tanto, no pueden usar su funcionalidad como una identificación, clave de autenticación y cifrado.

En la etapa 520, la aplicación de software personal 100 en el dispositivo informático personal 110 contacta con todos los servidores informáticos proveedores de datos participantes 120 que contienen datos de interés para el sujeto de datos, tales como registros de salud, registros de impuestos, registros de transacción, registros financieros, preferencias del consumidor - cualquier información que por naturaleza puede ser privada o sensible - y estos registros se almacenan en las bases de datos de aplicación 380. Este contacto se realizará usando la red de comunicaciones. Las direcciones electrónicas de los servidores informáticos proveedores de datos 120 pueden escribirse en una lista almacenada en el dispositivo informático personal 110 y accederse a ella por la aplicación de software personal 100, o la aplicación de software personal 100 puede contactar con un servidor web confiable (no mostrado) desde el que puede recuperar la lista más actualizada de direcciones electrónicas de servidores informáticos proveedores de datos participantes 120.

La aplicación de software personal 100 y la aplicación de software de intercambio de datos 125 en el uno o más

servidores informáticos proveedores de datos 120 están configuradas para intercambiar datos de forma segura entre sí. La aplicación de software de intercambio de datos 125 habrá sido desarrollada por el controlador de datos confiable. Esta es la primera vez que la aplicación de software personal 100 está contactando con el servidor informático proveedor de datos 120.

Después de establecer la conexión, la aplicación de software personal 100 transmite el nombre del sujeto de datos, datos de identificación personal, identificadores personales, términos de consentimiento opcionales, solicitud de acceso a datos opcional, preferencias personales opcionales y el identificador anónimo cifrado, a la aplicación de software de intercambio de datos 125 en el servidor informático proveedor de datos 120.

En la etapa 530, la aplicación de software de intercambio de datos 125 en el uno o más servidores informáticos proveedores de datos 120 recibe los datos de identificación transmitidos del sujeto de datos y los almacena en sus bases de datos de registro de usuario 370 ubicadas en el uno o más servidores informáticos proveedores de datos 120. Por lo tanto, la base de datos de registro de usuario 370 registrará el nombre del sujeto de datos, todos los identificadores personales, términos de consentimiento opcionales, solicitud de transferencia de datos opcional, preferencias de usuario opcionales y el identificador anónimo cifrado.

Una vez que ha concluido este proceso, la aplicación de software de intercambio de datos 125 transmite un mensaje a la aplicación de software personal 100 de que el proceso de registro ha concluido en ese servidor informático proveedor de datos específico 120.

A continuación, la aplicación de software personal 100 selecciona el siguiente servidor informático proveedor de datos en la lista de servidores informáticos proveedores de datos y reinicia el proceso de registro de usuario en todos los servidores informáticos proveedores de datos 120 hasta que el sujeto de datos se haya registrado como un nuevo usuario en todos los servidores informáticos proveedores de datos 120 en la lista.

La aplicación de software de intercambio de datos 125 busca las bases de datos de aplicación 380 en el uno o más servidores informáticos proveedores de datos 120 y usando el nombre del sujeto de datos e identificadores personales encuentra y recopila de las mismas todos los datos personales de interés asociados con el sujeto de datos identificado.

En la etapa 540, al encontrar los datos de interés y colocarlos en la memoria del servidor informático proveedor de datos 340, la aplicación de software de intercambio de datos 125 borra el nombre del sujeto de datos y cualquiera y todos los identificadores personales y los reemplaza con el identificador anónimo cifrado del sujeto de datos. Los datos de interés del sujeto se despojan, por lo tanto, de cualquier elemento de identificación personal y, por lo tanto, se anonimizan y se desidentifican.

En la etapa 550, la aplicación de software de intercambio de datos 125 en el uno o más servidores informáticos proveedores de datos 120 contacta a continuación con la aplicación de software de intercambio de datos 135 ubicada en el servidor informático de controlador de datos confiable 130 por medio de la red de comunicaciones. Una vez que se establece el contacto, la aplicación de software de intercambio de datos 125 en el servidor informático proveedor de datos 120 transmite los datos desidentificados del sujeto, información de interés anonimizada, los términos de consentimiento opcionales, solicitud de acceso y transferencia de datos opcional, preferencias de usuario opcionales y el identificador anónimo cifrado del sujeto de datos, a la aplicación de software de intercambio de datos 135 en el servidor informático de controlador de datos confiable 130. Las aplicaciones de software de intercambio de datos 125 registran los metadatos de transmisión (al menos la identidad de los ordenadores de comunicación y la indicación de tiempo del intercambio de datos) en el archivo de registro 390 en el uno o más servidores informáticos proveedores de datos 120.

Se observará que, el nombre y los identificadores personales del sujeto de datos no se transmiten al servidor informático de controlador de datos confiable 130. A continuación, la transmisión de datos de interés anonimizados se produce periódicamente, cada vez que se adquieran nuevos datos de interés-nuevos registros médicos, nuevos registros fiscales, nuevos registros financieros, etc. - por las bases de datos de aplicación 380 en el uno o más servidores informáticos proveedores de datos 120, mientras el consentimiento del sujeto de datos no se revoque en la aplicación de software personal 100 y se comunique a la aplicación de software de intercambio de datos 125. La aplicación de software de intercambio de datos 125 está configurada para realizar esta búsqueda periódica, para anonimizar y transmitir los datos de interés al servidor informático de controlador de datos confiable 130. Para transmitir únicamente información de interés reciente, la aplicación de software de intercambio de datos 125 se referirá a los metadatos de la transmisión anterior contenidos en el archivo de registro 390 y únicamente transmitirá información de interés adquirida desde ese evento.

En la etapa 560, el servidor de controlador de datos confiable 130 recibe los datos transmitidos desde el uno o más servidores informáticos proveedores de datos 120. La aplicación de software de intercambio de datos 135 registra los metadatos de transmisión (al menos la identidad de los ordenadores de comunicación y la indicación de tiempo del intercambio de datos) en el archivo de registro 490 en el servidor informático de controlador de datos confiable 130.

Al recibir el mensaje de datos desde el uno o más servidores informáticos proveedores de datos 120, la aplicación de

software de intercambio de datos 135 en el servidor informático de controlador de datos confiable 130 debe leer en primer lugar el identificador anónimo cifrado. En la realización general, el identificador anónimo se descifrará por el módulo de software criptográfico 401 usando el método correspondiente al método usado para cifrarlo originalmente. En la realización de clave asimétrica, el módulo de software criptográfico 401 lee el identificador anónimo cifrado del sujeto de datos y lo descifra usando la clave privada del servidor informático de controlador de datos confiable 130, obteniendo por tanto el identificador anónimo original del sujeto de datos, así como su clave pública.

En la etapa 570, el servidor informático de controlador de datos confiable 130 usa el identificador anónimo ahora descifrado para determinar si el sujeto de datos es nuevo o no. La aplicación de software de intercambio de datos 135 busca en la base de datos de registro de usuario 470 ubicada en el servidor informático de controlador de datos confiable 130 y compara el identificador anónimo recibido con los identificadores anónimos almacenados en la base de datos de registro de usuario 470.

En la etapa 575, si no se encuentra una coincidencia, a continuación, se registra una nueva entrada en la base de datos de registro de usuario 470 en el servidor informático de controlador de datos confiable 130, que incluye el identificador anónimo del sujeto de datos, términos de consentimiento opcionales, solicitud de transferencia de datos opcional, las preferencias de usuario opcionales y los metadatos de la transmisión se registran en un archivo de registro 490 ubicado en el servidor informático de controlador de datos confiable 130. El flujo de programa informático continúa a la etapa 580.

Si se encuentra una coincidencia o en el flujo de programa que continúa desde la etapa 575, a continuación, en la etapa 580, el sujeto de datos ya está registrado en la base de datos de registro de usuario 470 del servidor informático de controlador de datos confiable 130 y la aplicación de software de intercambio de datos 135 registra los datos de interés anonimizados del sujeto de datos en la base de datos de aplicación 480 del ordenador de controlador de datos confiable servidor 130, identificado solamente por el identificador anónimo del sujeto de datos.

Después de varios eventos de transmisión de datos, el servidor informático de controlador de datos confiable 130 almacenará una cantidad significativa de información personal anonimizada de interés que pertenece al sujeto de datos en su base de datos de aplicación 480. En consecuencia, el servidor informático de controlador de datos confiable 130, en ausencia de cualquier información de identificación personal acerca del sujeto de datos - sin nombre, sin identificadores personales, sin número de teléfono celular, sin dirección de correo electrónico - no tiene dirección para contactar y establecer comunicaciones con la aplicación de software personal 100 en el dispositivo informático personal del sujeto de datos 110 y devolver su información de interés obtenida periódicamente de múltiples servidores informáticos proveedores de datos 120. El servidor informático de controlador de datos confiable 130 no tiene los medios para contactar con el dispositivo informático personal 110 y volver a identificar al sujeto de datos y esto evita que un ordenador acceda a los datos personales identificados del sujeto de datos por accidente, negligencia o malicia. La divulgación presentada en la siguiente figura proporciona un sistema informático configurado para acceder y procesar los datos personales del sujeto de datos de una manera que no vulnera sus derechos de privacidad.

La figura 6 ilustra cómo se devuelven los datos de interés anonimizados a la aplicación de software personal 100 en el dispositivo informático personal 110 del sujeto de datos anónimo, una vez que todas las etapas 500 a 580 se han ejecutado con éxito.

En la etapa 600, es la aplicación de software personal 100 en el dispositivo informático personal 110 la que abre una sesión de comunicaciones con la aplicación de software de intercambio de datos 135 del servidor informático de controlador de datos confiable 130, a través de la red de comunicaciones. Esto es posible debido a que la aplicación de software personal 100 tiene la dirección electrónica del servidor informático de controlador de datos confiable 130 y está configurada para contactarlo periódicamente.

En la etapa 610, la aplicación de software personal 100 transmite una solicitud de intercambio de datos a la aplicación de software de intercambio de datos 135 del servidor informático de controlador de datos confiable 130, que comprende el identificador anónimo del sujeto de datos preferentemente cifrado en forma de una firma digital. La aplicación de software de intercambio de datos 135 registra los metadatos de la sesión de comunicaciones (identificador anónimo e indicación de tiempo) en el archivo de registro 490 en el servidor informático de controlador de datos confiable 130.

En la etapa 620, la aplicación de software de intercambio de datos 135 en el servidor informático de controlador de datos confiable 130 lee el identificador anónimo y su firma digital, si está presente, y debe determinar si es una solicitud válida.

En la etapa 630, la aplicación de software de intercambio de datos 135 busca en la base de datos de registro de usuario 470 ubicada en el servidor informático de controlador de datos confiable 130 y compara el identificador anónimo recibido con los identificadores anónimos almacenados en la base de datos de registro de usuario 470. Si es una firma digital, el módulo de software criptográfico 401 la verifica usando el identificador anónimo recibido como la clave de descifrado de la firma digital.

En la etapa 635, si no hay una coincidencia entre el identificador anónimo recibido y cualquier identificador anónimo almacenado, a continuación, el identificador anónimo recibido no es válido. En el caso de que la firma digital descifrada no sea idéntica al identificador anónimo recibido, la solicitud también no es válida. La aplicación de software de intercambio de datos 135 del servidor informático de controlador de datos confiable 130 deja de responder a la aplicación de software personal 100 en la sesión de comunicaciones.

En la etapa 640, si hay una coincidencia entre el identificador anónimo recibido y cualquier identificador anónimo almacenado, o si la firma digital descifrada coincide con el identificador anónimo recibido, a continuación, el identificador anónimo recibido y la solicitud de intercambio de datos son válidos.

La aplicación de software de intercambio de datos 135 busca en la base de datos de aplicación 480 en el servidor informático de controlador de datos confiable 130 datos de interés anonimizados identificados por el identificador anónimo validado y obtiene los datos de interés más recientes del sujeto de datos anónimo haciendo referencia al archivo de registro 490 que contiene la fecha de la sesión de comunicaciones anterior entre la aplicación de software personal del sujeto de datos 100 y la aplicación de software de intercambio de datos 135 en el servidor informático de controlador de datos confiable 130.

En la etapa 650, la aplicación de software de intercambio de datos 135 en el servidor informático de controlador de datos confiable 130 transmite la información de interés más reciente a la aplicación de software personal 100 en el dispositivo informático personal 110.

En la etapa 660, la aplicación de software personal 100 recibe la información de interés, la organiza y la almacena en la base de datos de información de interés 280 en el dispositivo informático personal 110 del sujeto de datos.

En la etapa 670, el sujeto de datos abre la aplicación de software personal 100 en su dispositivo informático personal 110 y consulta y usa la información de interés 280.

Se apreciará que, en el caso de información de interés que comprenda ficheros muy grandes, que es el caso cuando se transmiten imágenes y fotografías, los tiempos de transmisión pueden ser largos. Para acortar el tiempo de transferencia de un archivo grande de este tipo, la aplicación de software de intercambio de datos 135 en el servidor informático de controlador de datos confiable 130 puede transmitir una dirección de enlace bajo la cual el archivo se almacena en la base de datos de aplicación 480 del servidor informático de controlador de datos confiable 130, a la aplicación de software personal 100, en lugar del archivo grande. En esta realización, cada vez que el sujeto de datos desee consultar y usar estos archivos grandes, seleccionar la dirección de enlace en la aplicación de software personal 100 activa automáticamente la solicitud de intercambio de datos y el proceso de verificación de identificador anónimo descrito en las etapas 610 a 640 y el archivo grande se transmite realmente por la aplicación de software de intercambio de datos 135 en el servidor informático de controlador de datos confiable 130 a la base de datos de información de interés 280, para visualizarse en la aplicación de software personal 100. En una realización similar, este proceso de ahorro de ancho de banda puede usarse para todas las transmisiones normales de datos de interés entre la aplicación de software personal del sujeto de datos 100 y la aplicación de software de intercambio de datos 135 en el servidor informático de controlador de datos confiable 130.

Por lo tanto, el servidor informático de controlador de datos confiable 130 puede recopilar datos de interés anonimizados de múltiples servidores informáticos proveedores de datos 120 y transmitirlos a la aplicación de software personal 100 de su propietario legítimo, aunque anónimo. Esto representa un avance en la protección de los derechos de privacidad de los sujetos de datos cuando se intercambian datos personales.

A medida que la base de datos de aplicación 480 adquiere más información de interés de un gran número de sujetos de datos que ejecutan la aplicación de software personal 100 en sus dispositivos informáticos personales 110, y de todos los servidores informáticos proveedores de datos 120 participantes, el servidor informático de controlador de datos confiable 130 puede crear una base de datos de aplicaciones muy grande 480 y realizar un procesamiento informático a gran escala de datos anonimizados, usando técnicas tales como procesamiento estadístico, procesamiento de grandes cantidades de datos, aprendizaje automático e inteligencia artificial para obtener nueva información a partir de los datos almacenados, usando la aplicación de software de ciencia de datos 495. Esto será particularmente relevante en el caso de datos de salud y atención de la salud, establecer nuevas relaciones entre fármacos, tratamientos y terapias y cuantificar su impacto en cada individuo o clase de individuos, lo que conduce a una medicina de precisión usando datos del mundo real y una mejor salud individual y pública. Esto también será útil en el negocio de identificar las preferencias del consumidor, patrones de compra o interacciones sociales, del procesamiento a gran escala de datos personales, pero sin conocer el nombre del sujeto de datos. Tal procesamiento útil únicamente será posible si se recopilan grandes cantidades de datos personales en los ordenadores. La presente invención permite una acumulación tan grande de datos personales de una manera que evita que los ordenadores que los procesan asocien los datos con una persona identificada y, por lo tanto, resuelve el problema de proteger los derechos de privacidad de las personas cuyos datos personales se procesan por esos ordenadores.

Aunque se han ilustrado realizaciones particulares del sistema y método de la presente invención en los dibujos adjuntos y se han descrito en la descripción detallada anterior, se entenderá que la invención no se limita a las

realizaciones divulgadas, en concreto, en el uso de más o menos medios criptográficos y múltiples combinaciones de los mismos, pero es capaz de numerosas reorganizaciones, modificaciones y sustituciones sin alejarse del alcance de la invención.

REIVINDICACIONES

1. Un método para ejecutar un proceso de inicio de sesión para un sujeto de datos a un servidor informático de controlador de datos confiable (130) usando una aplicación de software personal (100) instalada en un dispositivo informático personal (110) del sujeto de datos, en el que el sujeto de datos se identifica a sí mismo exclusivamente a través de un identificador anónimo cifrado, y para devolver información de interés por el servidor informático de controlador de datos confiable (130) al sujeto de datos a su aplicación de software personal (100), que comprende las etapas:

a. El sujeto de datos descarga e instala la aplicación de software personal (100) y un módulo de software criptográfico (101) en su dispositivo informático personal (110) e introduce al menos el nombre de la persona y los identificadores personales y el consentimiento opcional,
b. El módulo de software criptográfico (101) en el dispositivo informático personal (110) genera un identificador anónimo y una versión cifrada del identificador anónimo,
c. La aplicación de software personal (100) en el dispositivo informático personal (110) contacta con una aplicación de software de intercambio de datos (125) en uno o más servidores informáticos proveedores de datos (120) que almacenan datos relacionados con el sujeto de datos, estando la aplicación de software personal (100) y la aplicación de software de intercambio de datos (125) configuradas para intercambiar datos de forma segura, y transmite el nombre del sujeto de datos, identificadores personales, el identificador anónimo cifrado y el consentimiento opcional a la aplicación de software de intercambio de datos (125) que recibe el nombre del sujeto de datos, identificadores personales, el identificador anónimo cifrado y el consentimiento opcional,
d. La aplicación de software de intercambio de datos (125) del uno o más servidores informáticos proveedores de datos (120) recibe y registra al menos el nombre del sujeto de datos, identificadores personales e identificador anónimo cifrado y consentimiento opcional y busca en las bases de datos de aplicación (380) del servidor informático proveedor de datos (120) datos relacionados con el sujeto de datos, por medio del nombre del sujeto de datos y los identificadores personales,
e. Al encontrar los datos relacionados con el sujeto de datos, en lo sucesivo en el presente documento denominados como los datos de interés, la aplicación de software de intercambio de datos (125) del uno o más servidores informáticos proveedores de datos (120) crea un mensaje al que añade los datos de interés, el identificador anónimo cifrado del sujeto de datos y elimina el nombre del sujeto de datos y todos los identificadores personales para anonimizar los datos de interés,
f. La aplicación de software de intercambio de datos (125) del uno o más servidores informáticos proveedores de datos (120) transmite el mensaje que contiene los datos de interés anonimizados identificados únicamente por el identificador anónimo cifrado del sujeto de datos al servidor informático de controlador de datos confiable (130),
g. La aplicación de software de intercambio de datos (135) en el servidor informático de controlador de datos confiable (130), que está configurada para intercambiar datos de forma segura con la aplicación de intercambio de datos (125) de uno o más servidores informáticos proveedores de datos (120), recibe el mensaje y lo lee, descifra el identificador anónimo cifrado para obtener el identificador anónimo original, verifica si el identificador anónimo ya está registrado en una base de datos de registro de usuario (470) ubicada en el servidor informático de controlador de datos confiable (130) y

i. Al no encontrarlo, registra el identificador anónimo como un nuevo usuario en la base de datos de registro de usuarios (470), registra el identificador anónimo y los metadatos de mensaje en un archivo de registro (490) y almacena los al menos datos de interés anonimizados del sujeto de datos y el identificador anónimo en una base de datos de aplicación (480), identificándose los datos de interés anonimizados únicamente por el identificador anónimo del sujeto de datos, o
ii. Al encontrarlo, registra el identificador anónimo y los metadatos de mensaje en un archivo de registro (490) y almacena los al menos datos de interés anonimizados del sujeto de datos en una base de datos de aplicación (480), identificados únicamente por el identificador anónimo del sujeto de datos,

h. La transmisión de datos de interés anonimizados se produce periódicamente entre las aplicaciones de software de intercambio de datos (125) del uno o más servidores informáticos proveedores de datos (120) y la aplicación de software de intercambio de datos (135) del servidor informático de controlador de datos confiable (130) de modo que se añaden continuamente nuevos datos de interés anonimizados relacionados con el mismo sujeto de datos a la base de datos de aplicación (480) en el servidor informático de controlador de datos confiable (130),
i. La aplicación de software personal (100) en el dispositivo informático personal (110) del sujeto de datos y la aplicación de software de intercambio de datos (135) del servidor informático de controlador de datos confiable (130), que están configuradas para comunicarse de forma segura entre sí, establecen comunicación y la aplicación de software de intercambio de datos (135) del servidor informático de controlador de datos confiable (130) transmite los datos de interés anonimizados a la aplicación de software personal (100) en el dispositivo informático personal (110) devolviendo de esta manera los datos anonimizados al sujeto de datos anónimo,

en donde la transmisión de los datos de interés anonimizados entre el servidor informático de controlador de datos confiable (130) y el dispositivo informático personal (110) del sujeto de datos anónimo se produce por medio de una sesión de comunicaciones siempre iniciada por la aplicación de software personal (100) en el dispositivo informático personal (110) del sujeto de datos, para conectarse a la dirección electrónica conocida del servidor informático de

controlador de datos confiable (130) y la aplicación de software de intercambio de datos (135) en el servidor informático de controlador de datos confiable (130) debe esperar a que la aplicación de software personal (100) inicie la sesión de comunicaciones, impidiendo que el servidor informático de controlador de datos confiable (130) inicie una sesión de comunicación de este tipo en ausencia de cualquier información acerca del nombre del sujeto de datos, identificadores personales o dirección electrónica del dispositivo informático personal (110).

2. El método de la reivindicación 1, en donde la sesión de comunicaciones entre la aplicación de software personal (100) en el dispositivo informático personal (110) del sujeto de datos y la aplicación de software de intercambio de datos (135) en el servidor informático de controlador de datos confiable (130) se inicia por la aplicación de software personal (100) transmitiendo una solicitud de intercambio de datos identificada exclusivamente por el identificador anónimo del sujeto de datos o por firma digital, recibiendo la aplicación de software de intercambio de datos (135) la solicitud de intercambio de datos y confirmando que se ha recibido una solicitud válida y que el identificador anónimo almacenado y el identificador anónimo recibido corresponden al mismo sujeto de datos anónimo.

3. El método de la reivindicación 1, en donde el identificador anónimo se genera como una clave pública asimétrica por un módulo de software criptográfico (101) en el dispositivo informático personal (110), que se deriva de una clave criptográfica privada generada aleatoriamente, y se cifra usando el módulo de software criptográfico (101) por medio de la clave criptográfica pública conocida del servidor informático de controlador de datos confiable (130), y la aplicación de software personal (100) transmite el al menos el nombre del sujeto de datos, identificadores personales y el identificador anónimo cifrado a cada servidor informático proveedor de datos (120), la aplicación de software de intercambio de datos (125) en el uno o más servidores informáticos proveedores de datos (120) que lo recibe e incluye el identificador anónimo cifrado en el mensaje que contiene los datos de interés anonimizados, transmitiéndolo a la aplicación de software de intercambio de datos (135) del servidor informático de controlador de datos confiable (130), un módulo de software criptográfico (101) en el servidor informático de controlador de datos confiable (130) que recibe y descifra el identificador anónimo cifrado por medio de la clave criptográfica privada del servidor informático de controlador de datos confiable (130).

4. El método de la reivindicación 1, en donde el identificador anónimo es una clave de identificación, una clave de autenticación y una clave criptográfica.

5. El método de la reivindicación 1, en donde los módulos de software criptográfico que cifran las comunicaciones entre el dispositivo informático personal del sujeto de datos (110), el uno o más servidores informáticos proveedores de datos (120) y los servidores informáticos de controlador de datos confiable (130) usan claves criptográficas asimétricas, preferentemente empleando el algoritmo de firma digital de curva elíptica.

6. El método de la reivindicación 1, en donde la aplicación de software personal (100) en el dispositivo informático personal (110) del sujeto de datos abre una sesión de comunicaciones con la aplicación de software de intercambio de datos (135) en el servidor informático de controlador de datos confiable (130) a intervalos de tiempo predeterminados configurados en la aplicación de software personal (100) o a intervalos de tiempo preferidos configurados por el sujeto de datos o en cualquier momento por orden del sujeto de datos.

7. El método de la reivindicación 1, en donde la transmisión de mensajes que contienen datos de interés anonimizados desde el uno o más servidores informáticos proveedores de datos (120) al servidor informático de controlador de datos confiable (130), o el registro de un nuevo sujeto de datos anónimo en la base de datos de registro de usuario del controlador de datos confiable (470), o la comunicación de datos de interés anonimizados desde el controlador de datos confiable (130) al dispositivo informático personal (110) del sujeto de datos, se produce sin que el sujeto de datos emplee un nombre de usuario definido por el usuario y una contraseña de sistema convencionales almacenados en cualquiera de los servidores informáticos (120, 130) y la verificación de la identidad del sujeto de datos por la aplicación de software de intercambio de datos (135) en el servidor informático de controlador de datos confiable (130) se logra únicamente por medio del identificador anónimo del sujeto de datos.

8. El método de la reivindicación 1, en donde los datos personales del sujeto de datos se recopilan de las bases de datos de aplicación (380) en el uno o más servidores informáticos proveedores de datos (120), se anonimizan y se transmiten a un servidor informático de controlador de datos confiable (130), donde se recopilan y organizan bajo la identidad del identificador anónimo del sujeto de datos y se devuelven a la aplicación de software personal (100) en el dispositivo informático personal (110) del sujeto de datos por la aplicación de software de intercambio de datos (135) en el servidor informático de controlador de datos confiable (130).

9. Un medio informático no transitorio que almacena código fuente, que, cuando se ejecuta por un procesador, realiza un método para ejecutar un proceso de inicio de sesión para un sujeto de datos a un servidor informático de controlador de datos confiable (130) usando una aplicación de software personal (100) instalada en un dispositivo informático personal (110) del sujeto de datos, en el que el sujeto de datos se identifica a sí mismo exclusivamente a través de un identificador anónimo cifrado, y para devolver información de interés por el servidor informático de controlador de datos confiable (130) al sujeto de datos a su aplicación de software personal (100), que comprende las etapas:

a. El sujeto de datos descarga e instala la aplicación de software personal (100) y un módulo de software

criptográfico (101) en su dispositivo informático personal (110) e introduce al menos el nombre de la persona y los identificadores personales y el consentimiento opcional,

b. El módulo de software criptográfico (101) en el dispositivo informático personal (110) genera un identificador anónimo y una versión cifrada del identificador anónimo,

c. La aplicación de software personal (100) en el dispositivo informático personal (110) contacta con una aplicación de software de intercambio de datos (125) en uno o más servidores informáticos proveedores de datos (120) que almacenan datos relacionados con el sujeto de datos, estando la aplicación de software personal (100) y la aplicación de software de intercambio de datos (125) configuradas para intercambiar datos de forma segura, y transmite el nombre del sujeto de datos, identificadores personales, el identificador anónimo cifrado y el consentimiento opcional a la aplicación de software de intercambio de datos (125) que recibe el nombre del sujeto de datos, identificadores personales, el identificador anónimo cifrado y el consentimiento opcional,

d. La aplicación de software de intercambio de datos (125) del uno o más servidores informáticos proveedores de datos (120) recibe y registra al menos el nombre del sujeto de datos, identificadores personales e identificador anónimo cifrado y consentimiento opcional y busca en las bases de datos de aplicación (380) del servidor informático proveedor de datos (120) datos relacionados con el sujeto de datos, por medio del nombre del sujeto de datos y los identificadores personales,

e. Al encontrar los datos relacionados con el sujeto de datos, en lo sucesivo en el presente documento denominados como los datos de interés, la aplicación de software de intercambio de datos (125) del uno o más servidores informáticos proveedores de datos (120) crea un mensaje al que añade los datos de interés, el identificador anónimo cifrado del sujeto de datos y elimina el nombre del sujeto de datos y todos los identificadores personales para anonimizar los datos de interés,

f. La aplicación de software de intercambio de datos (125) del uno o más servidores informáticos proveedores de datos (120) transmite el mensaje que contiene los datos de interés anonimizados identificados únicamente por el identificador anónimo cifrado del sujeto de datos al servidor informático de controlador de datos confiable (130),

g. La aplicación de software de intercambio de datos (135) en el servidor informático de controlador de datos confiable (130), que está configurada para intercambiar datos de forma segura con la aplicación de intercambio de datos (125) de uno o más servidores informáticos proveedores de datos (120), recibe el mensaje y lo lee, descifra el identificador anónimo cifrado para obtener el identificador anónimo original, verifica si el identificador anónimo ya está registrado en una base de datos de registro de usuario (470) ubicada en el servidor informático de controlador de datos confiable (130) y

i. Al no encontrarlo, registra el identificador anónimo como un nuevo usuario en la base de datos de registro de usuarios (470), registra el identificador anónimo y los metadatos de mensaje en un archivo de registro (490) y almacena los al menos datos de interés anonimizados del sujeto de datos y el identificador anónimo en una base de datos de aplicación (480), identificándose los datos de interés anonimizados únicamente por el identificador anónimo del sujeto de datos, o

ii. Al encontrarlo, registra el identificador anónimo y los metadatos de mensaje en un archivo de registro (490) y almacena los al menos datos de interés anonimizados del sujeto de datos en una base de datos de aplicación (480), identificados únicamente por el identificador anónimo del sujeto de datos,

h. La transmisión de datos de interés anonimizados se produce periódicamente entre las aplicaciones de software de intercambio de datos (125) del uno o más servidores informáticos proveedores de datos (120) y la aplicación de software de intercambio de datos (135) del servidor informático de controlador de datos confiable (130) de modo que se añaden continuamente nuevos datos de interés anonimizados relacionados con el mismo sujeto de datos a la base de datos de aplicación (480) en el servidor informático de controlador de datos confiable (130),

i. La aplicación de software personal (100) en el dispositivo informático personal (110) del sujeto de datos y la aplicación de software de intercambio de datos (135) del servidor informático de controlador de datos confiable (130), que están configuradas para comunicarse de forma segura entre sí, establecen comunicación y la aplicación de software de intercambio de datos (135) del servidor informático de controlador de datos confiable (130) transmite los datos de interés anonimizados a la aplicación de software personal (100) en el dispositivo informático personal (110) devolviendo de esta manera los datos anonimizados al sujeto de datos anónimo,

en donde la transmisión de los datos de interés anonimizados entre el servidor informático de controlador de datos confiable (130) y el dispositivo informático personal (110) del sujeto de datos anónimo se produce por medio de una sesión de comunicaciones siempre iniciada por la aplicación de software personal (100) en el dispositivo informático personal (110) del sujeto de datos, para conectarse a la dirección electrónica conocida del servidor informático de controlador de datos confiable (130) y la aplicación de software de intercambio de datos (135) en el servidor informático de controlador de datos confiable (130) debe esperar a que la aplicación de software personal (100) inicie la sesión de comunicaciones, impidiendo que el servidor informático de controlador de datos confiable (130) inicie una sesión de comunicación de este tipo en ausencia de cualquier información acerca del nombre del sujeto de datos, identificadores personales o dirección electrónica del dispositivo informático personal (110).

10. Un sistema informático para la anonimización de datos, comprendiendo el sistema informático:

a. un dispositivo informático personal (110) que tiene un módulo de software criptográfico (101) configurado para generar un identificador anónimo del usuario y una versión cifrada del mismo;

b. una pluralidad de servidores informáticos proveedores de datos (120) configurados para recibir datos personales desde el dispositivo informático personal (110), incluyendo el nombre del usuario y el identificador anónimo cifrado, almacenar los datos personales en una base de datos de registro de usuario (370), buscar en bases de datos de aplicación (380) datos de usuario, y reemplazar el nombre del usuario con el identificador anónimo cifrado para crear datos anonimizados; y

c. un servidor informático de controlador de datos confiable (130) configurado para recibir los datos anonimizados y un identificador anónimo cifrado de la pluralidad de servidores informáticos proveedores de datos (120);

en donde el servidor informático de controlador de datos confiable (130) está configurado para esperar una solicitud de intercambio de datos válida desde la aplicación de software personal (100) del dispositivo informático personal (110) identificada por el identificador anónimo del usuario y para responder a la misma con datos de interés anónimos.

Fig. 1a

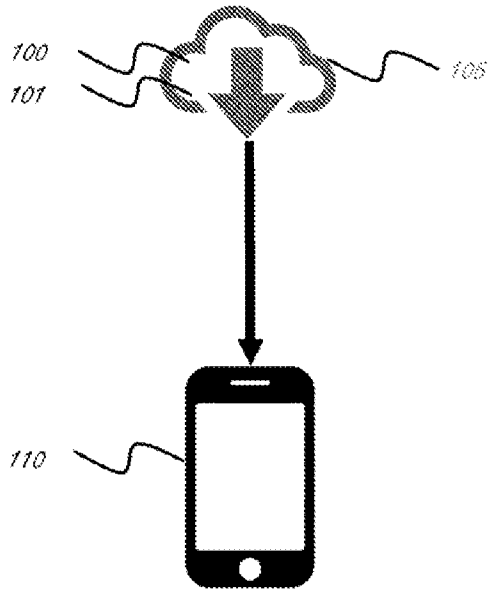


Fig. 1b

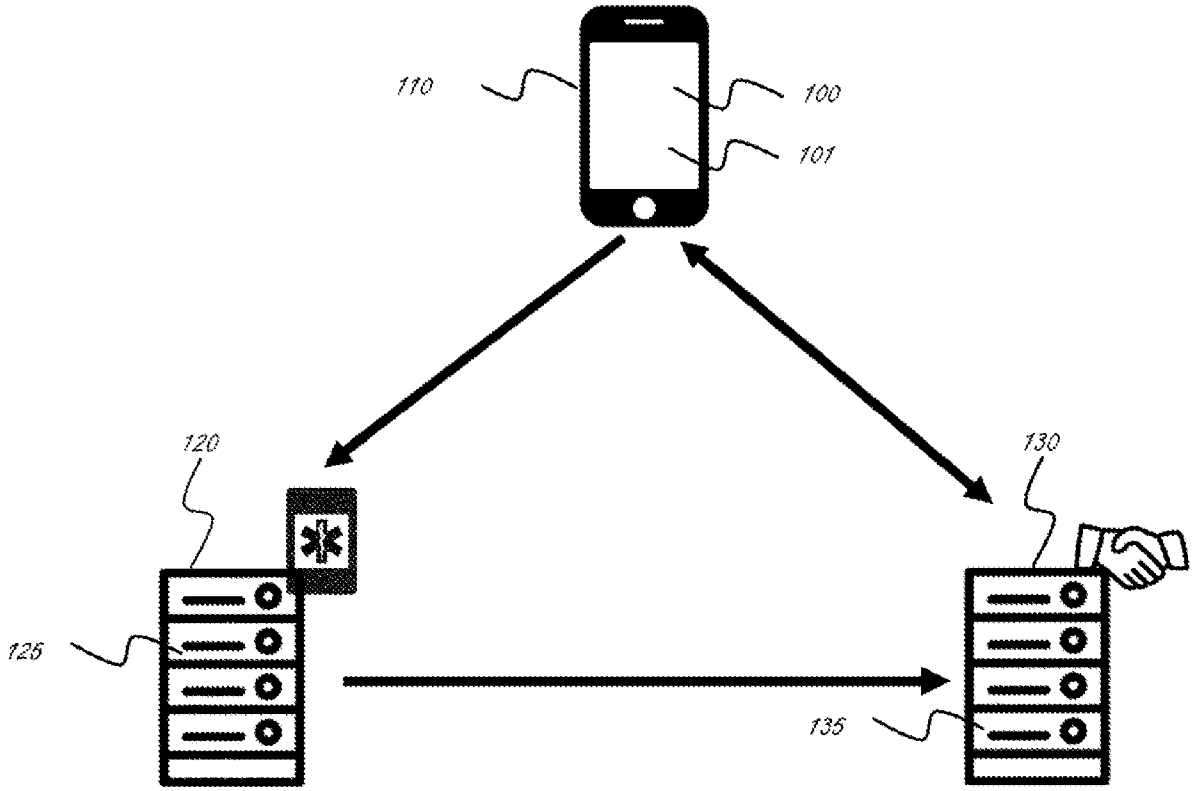


Fig. 2

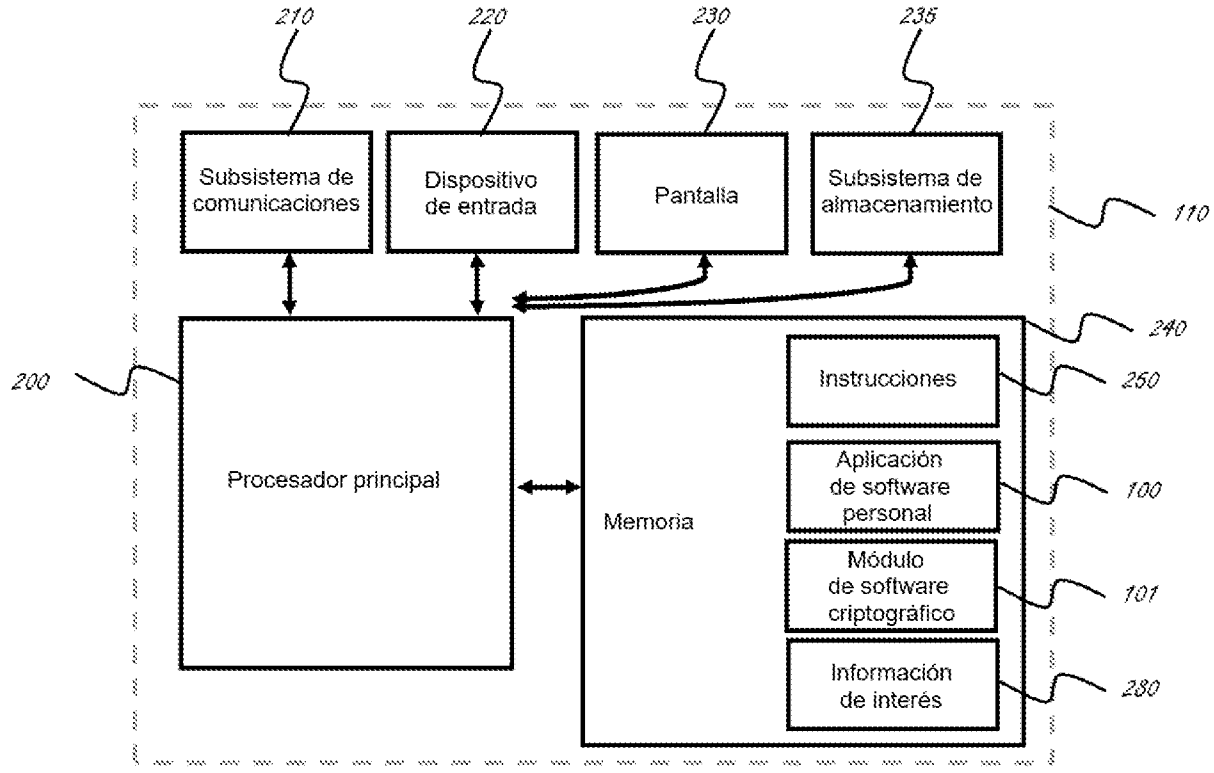

210
220
230
235
Subsistema de comunicaciones
Dispositivo de entrada
Pantalla
Subsistema de almacenamiento
110
240
200
Procesador principal
Memoria
Instrucciones
250
Aplicación de software personal
100
Módulo de software criptográfico
101
Información de interés
280

Fig. 3

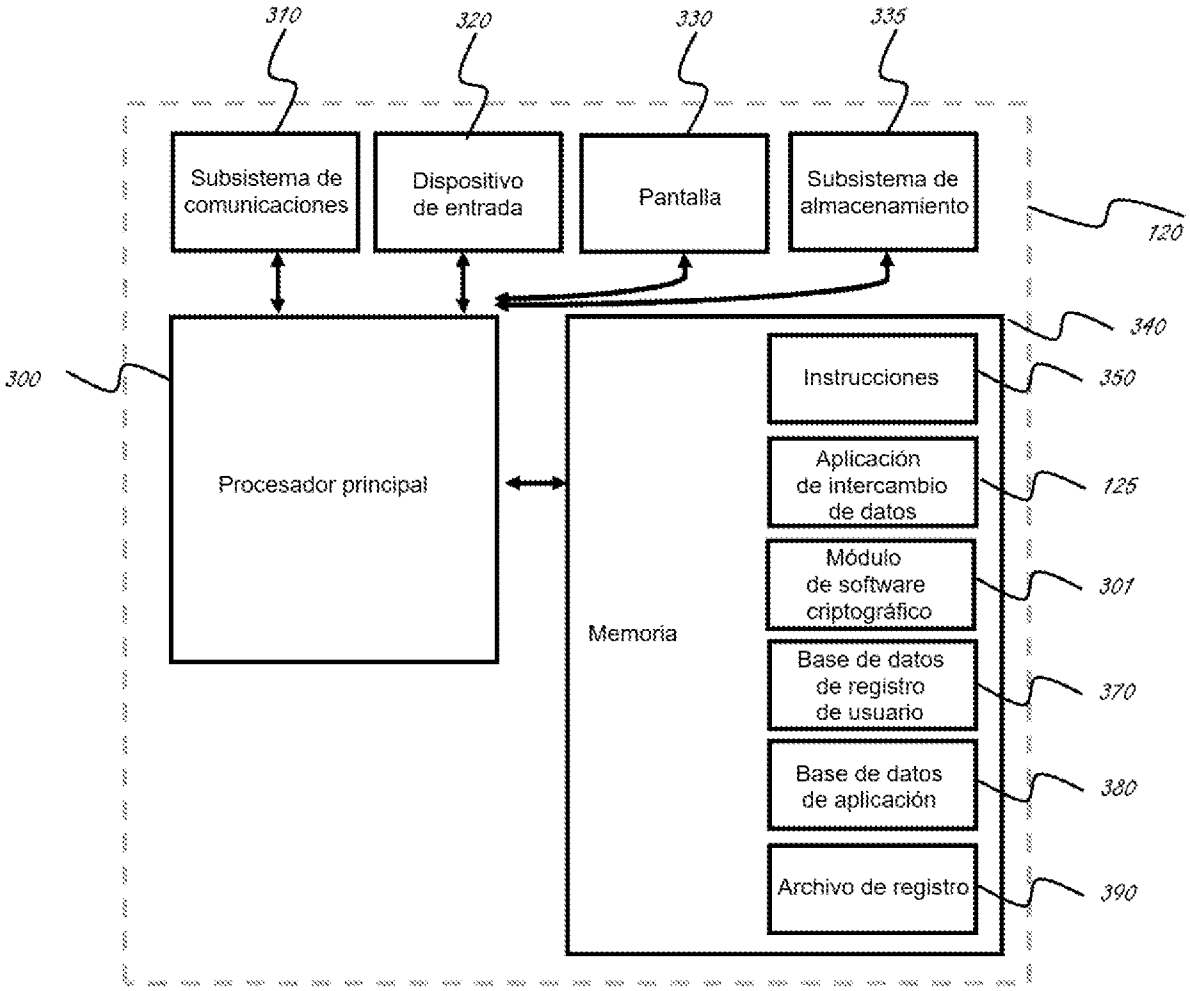

310
320
330
335
Subsistema de comunicaciones
Dispositivo de entrada
Pantalla
Subsistema de almacenamiento
120
340
300
Procesador principal
Memoria
Instrucciones
350
Aplicación de intercambio de datos
125
Módulo de software criptográfico
301
Base de datos de registro de usuario
370
Base de datos de aplicación
380
Archivo de registro
390

Fig. 4

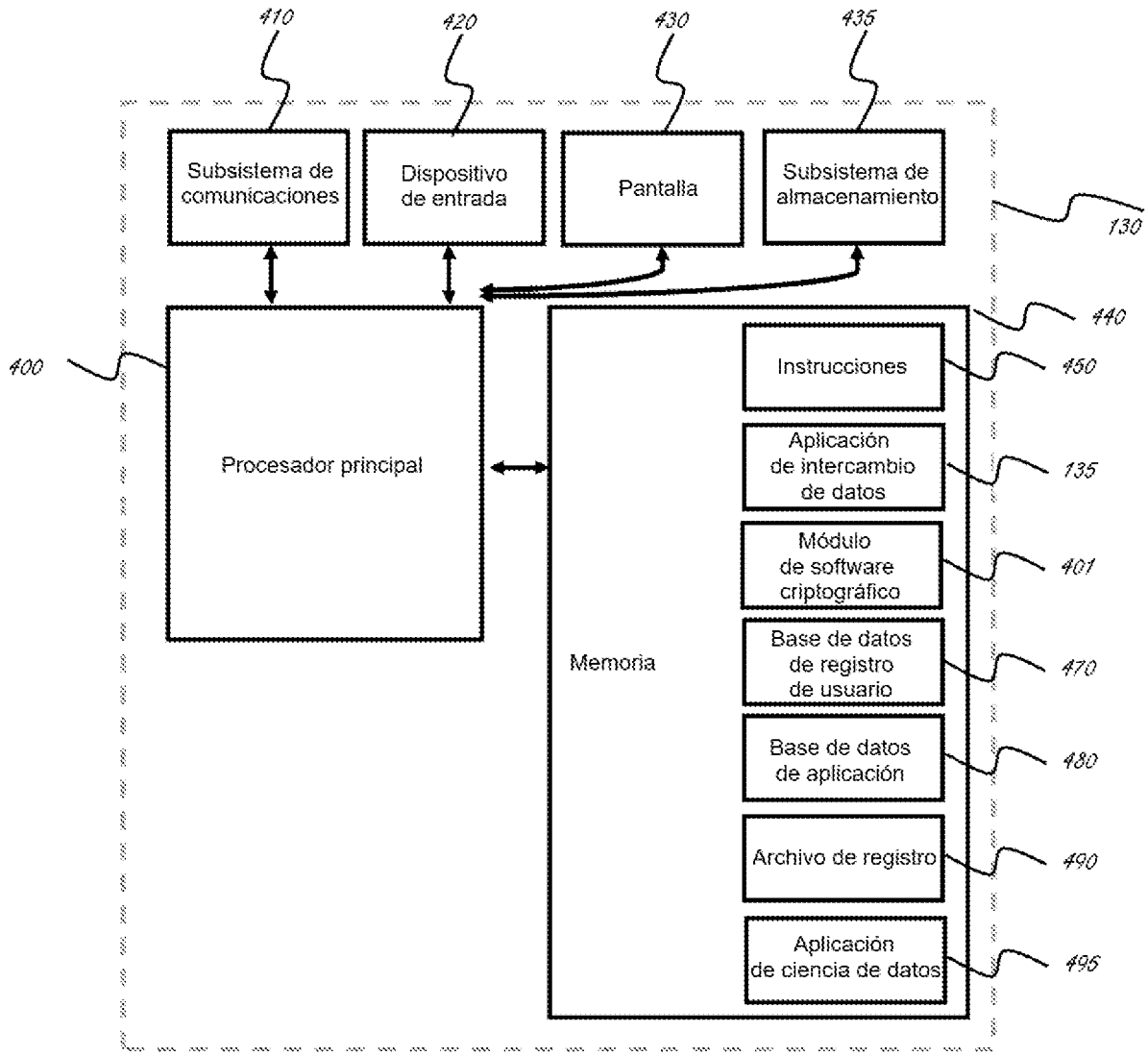

410
420
430
435
Subsistema de comunicaciones
Dispositivo de entrada
Pantalla
Subsistema de almacenamiento
130
440
400
Procesador principal
Memoria
Instrucciones
450
Aplicación de intercambio de datos
135
Módulo de software criptográfico
401
Base de datos de registro de usuario
470
Base de datos de aplicación
480
Archivo de registro
490
Aplicación de ciencia de datos
495

Fig. 5

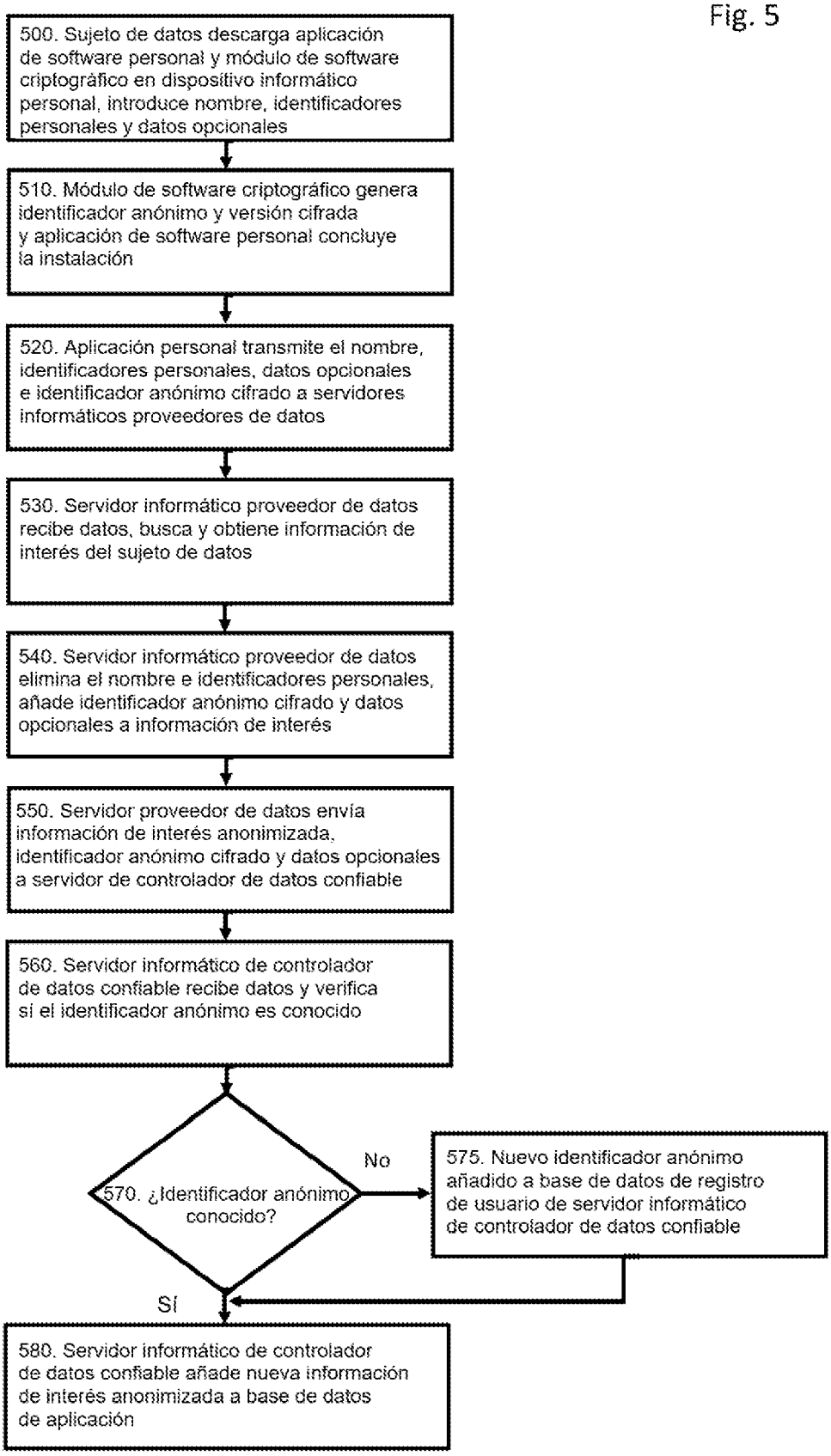
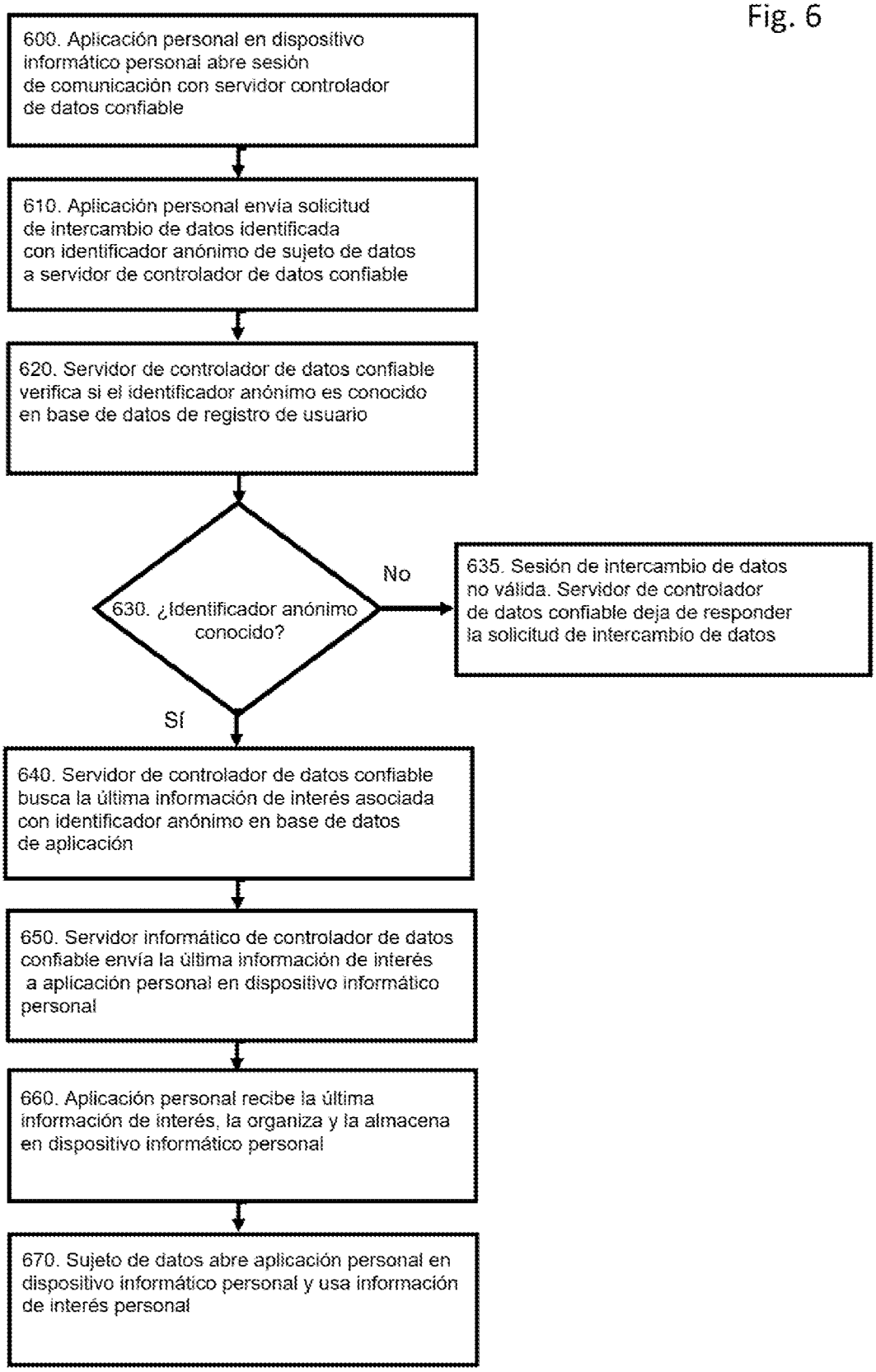

500. Sujeto de datos descarga aplicación de software personal y módulo de software criptográfico en dispositivo informático personal, introduce nombre, identificadores personales y datos opcionales
510. Módulo de software criptográfico genera identificador anónimo y versión cifrada y aplicación de software personal concluye la instalación
520. Aplicación personal transmite el nombre, identificadores personales, datos opcionales e identificador anónimo cifrado a servidores informáticos proveedores de datos
530. Servidor informático proveedor de datos recibe datos, busca y obtiene información de interés del sujeto de datos
540. Servidor informático proveedor de datos elimina el nombre e identificadores personales, añade identificador anónimo cifrado y datos opcionales a información de interés
550. Servidor proveedor de datos envía información de interés anonimizada, identificador anónimo cifrado y datos opcionales a servidor de controlador de datos confiable
560. Servidor informático de controlador de datos confiable recibe datos y verifica si el identificador anónimo es conocido
570. ¿Identificador anónimo conocido?
No
575. Nuevo identificador anónimo añadido a base de datos de registro de usuario de servidor informático de controlador de datos confiable
Sí
580. Servidor informático de controlador de datos confiable añade nueva información de interés anonimizada a base de datos de aplicación

Fig. 6


600. Aplicación personal en dispositivo informático personal abre sesión de comunicación con servidor controlador de datos confiable
610. Aplicación personal envía solicitud de intercambio de datos identificada con identificador anónimo de sujeto de datos a servidor de controlador de datos confiable
620. Servidor de controlador de datos confiable verifica si el identificador anónimo es conocido en base de datos de registro de usuario
630. ¿Identificador anónimo conocido?
No
635. Sesión de intercambio de datos no válida. Servidor de controlador de datos confiable deja de responder la solicitud de intercambio de datos
Sí
640. Servidor de controlador de datos confiable busca la última información de interés asociada con identificador anónimo en base de datos de aplicación
650. Servidor informático de controlador de datos confiable envía la última información de interés a aplicación personal en dispositivo informático personal
660. Aplicación personal recibe la última información de interés, la organiza y la almacena en dispositivo informático personal
670. Sujeto de datos abre aplicación personal en dispositivo informático personal y usa información de interés personal