EUROPEAN UNION AGENCY
FOR CYBERSECURITY

INGENIERÍA DE COMPARTICIÓN DE DATOS PERSONALES

Casos de uso y tecnologías emergentes

ENERO 2023

SOBRE ENISA

La Agencia de Ciberseguridad de la Unión Europea, ENISA es la agencia de la Unión dedicada a lograr un alto nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada por el Reglamento sobre la Ciberseguridad de la UE, la Agencia de Ciberseguridad de la Unión Europea contribuye a la ciberpolítica e la UE, mejora la fiabilidad de los productos, servicios y procesos de las TIC con sistemas de certificación de la ciberseguridad, coopera con los Estados miembros y los organismos de la UE y ayuda a Europa a prepararse para los retos cibernéticos del mañana. Mediante el intercambio de conocimientos, el desarrollo de capacidades y la sensibilización, la Agencia colabora con sus principales interesados para reforzar la confianza en la economía conectada, impulsar la resistencia de las infraestructuras de la Unión y, en última instancia, mantener la seguridad digital de la sociedad y los ciudadanos europeos. Más información sobre ENISA y su trabajo en: www.enisa.europa.eu.

CONTACTO

Para ponerse en contacto con los autores, utilice isdp@enisa.europa.eu
Para consultas de los medios de comunicación sobre este documento, utilice press@enisa.europa.eu.

COLABORADORES

Isabel Barbera, Claude Castelluccia, Giuseppe D'acquisto, Marta Fydrych Gasowska, Marit Hansen, Jaap-Henk Hoepman, Meiko Jensen, Konstantinos Limniotis, Maria Raphael, Marie-Charlotte Roques Bonnet, Fernando Silva, Fatbardh Veseli, Barbara Vieira, Kim Wuyts, Christian Zimmermann, Luis de Salvador Carrasco, Peter Kraus, Stephanie Mihail, Miguel Peñalba Moldes y Prokopios Drogkaris

EDITORES

Prokopios Drogkaris (ENISA), Monika Adamczyk (ENISA)

AGRADECIMIENTOS

Agradecemos a Kristof Verslype su revisión y sus valiosos comentarios.

AVISO LEGAL

AVISO SOBRE DERECHOS DE AUTOR

ISBN 978-92-9204-602-6, DOI 10.2824/36813

ÍNDICE

RESUMEN EJECUTIVO

En los últimos veinte años, hemos experimentado un aumento constante de la cantidad de datos que se generan y, posteriormente, se procesan de alguna manera. Los datos han pasado de ser un recurso escaso, difícil de recopilar y gestionar de forma centralizada, a convertirse en un recurso abundante creado de forma descentralizada y fácil de reproducir y comunicar. Parece existir una tendencia natural a “sacar los datos de los dispositivos o las organizaciones” y compartirlos entre distintas partes para crear nuevo valor para nuestra sociedad, o simplemente para reducir los costes operativos.

La compartición de datos puede considerarse como la divulgación de datos a terceros ajenos a la organización con el fin de lograr un propósito específico. Esta compartición puede llevarse a cabo como parte de una operación de tratamiento o al intentar proporcionar una utilidad adicional a los datos existentes. Las recientes iniciativas legislativas de la UE que promueven la compartición de datos son instrumentos sectoriales o intersectoriales que pretenden hacer que los datos estén disponibles regulando la reutilización de datos de titularidad pública y privada, incluidos los datos personales. También facilitan la compartición de datos mediante la creación de intermediarios y entornos de intercambio novedosos en los que las partes implicadas pueden compartir datos e instalaciones de forma fiable y segura.

Este informe pretende analizar con detalle casos de uso específicos relacionados con la compartición de datos personales, principalmente en el sector sanitario, y analiza cómo las tecnologías específicas y las consideraciones de implementación pueden apoyar el cumplimiento de las especificaciones de protección de datos. Tras analizar algunos de los retos de la compartición de datos (personales), este informe muestra cómo diseñar tecnologías y técnicas específicas que permitan compartir datos y preservar la privacidad.

Más específicamente, se analizan casos concretos de intercambio de datos en el sector sanitario, con el objetivo de demonstrar cómo pueden cumplirse los principios de protección de datos mediante el uso adecuado de soluciones tecnológicas basadas en técnicas criptográficas avanzadas. A continuación, analiza la compartición de datos que tiene lugar como parte de otro proceso o servicio, en el que los datos se procesan mediante algún canal o entidad secundarios antes de llegar a su destinatario principal. Por último, identifica retos, consideraciones y posibles arquitecturas como soluciones a aspectos de control por parte de los interesados (como el derecho de supresión y el derecho de rectificación al compartir datos).

1. INTRODUCCIÓN

Los datos están en el centro de nuestra vida cotidiana y de nuestra economía. En los últimos veinte años, hemos experimentado un aumento constante de la cantidad de datos que se generan y, posteriormente, se procesan de alguna manera. Los datos han pasado de ser un recurso escaso, difícil de recopilar y gestionado de forma centralizada y costoso de almacenar, transmitir y procesar, a convertirse en un recurso abundante creado de forma descentralizada (por individuos o por sensores) fácil de replicar y de comunicar o difundir a escala. Esto se hace patente por el hecho de que en los últimos 20 años la capacidad de la fibra óptica troncal de Internet se ha multiplicado casi por 100 (de 10 Gbps a casi 1 Tbps), mientras que el coste de transmisión de un solo Gbps ha disminuido al mismo ritmo, situándose hoy en día en torno al 1% del coste incurrido a principios de 2000 [1].

Existe una tendencia natural a "extraer datos de los dispositivos o las organizaciones" y compartirlos entre distintas partes para crear nuevo valor.

Los datos se consideran la nueva moneda y las organizaciones intercambian información sobre sus clientes con sus socios, plataformas analíticas, administraciones públicas y otras partes interesadas del ecosistema del dato con el fin de aprovechar las nuevas tecnologías o la información adicional que pueden obtener de la compartición y la correlación. Parece existir una tendencia natural a "sacar los datos de los dispositivos o las organizaciones" y compartirlos entre distintas partes para crear nuevo valor para nuestra sociedad, o simplemente para reducir los costes operativos[1]. Compartir datos ya empieza a ser la norma y no una excepción en el tratamiento de datos. Para hacer uso del valor de los datos, los proveedores de servicios tienen que ser capaces de utilizarlos, incluidos los que poseen otros.

Tratando de proporcionar una descripción precisa, y basándose en las definiciones proporcionadas por la Comisión de Protección de datos (DPC) en 2019 [2] y la ICO en 2020 [3], la compartición de datos puede considerarse como la divulgación de datos a terceros ajenos a la organización con el fin de lograr un propósito específico. Dicha compartición puede llevarse a cabo como parte de una operación de tratamiento o para intentar proporcionar una utilidad adicional a los datos existentes. La compartición de datos puede hacerse de forma rutinaria o en respuesta a situaciones específicas o de emergencia. Según Gartner [4], compartir datos es una necesidad empresarial, ya que puede potenciar la transformación digital y la innovación.

1.1 INICIATIVAS LEGISLATIVAS PERTINENTES DE LA UE

Actualmente, los legisladores europeos tienen un gran interés en la compartición de datos. Uno de los pilares fundamentales de la Estrategia europea de datos [5] es aumentar la disponibilidad de datos y facilitar su compartición entre sectores y países de la UE para aprovechar el potencial de los datos en beneficio de los ciudadanos y las empresas europeas. Considerando únicamente la zona de la UE 27, el valor de los datos para la economía previsto para 2025 será de 829.000 millones de euros, frente a los 301.000 millones de euros (2,4% del PIB de la UE) en 2018.[2] Se espera que facilitar el acceso a los datos y su compartición aporte beneficios importantes y concretos en diversos ámbitos, como el diagnóstico personalizado y la telemedicina, los transportes, la elaboración de políticas y la administración pública.

La Reglamento Europea de Gobernanza de Datos [6] prevé mecanismos para aumentar la disponibilidad de datos en el sector público y superar los obstáculos técnicos a la reutilización de datos de interés público. Estos mecanismos se apoyan en un conjunto de medidas concretas que facilitan la compartición de datos. Las medidas incluyen el establecimiento de intermediarios de datos que funcionen como organizadores fiables de datos y tecnologías

[1] IDC, *Data Age 2025 - The digitization of the world, from edge to core*, Nov. 2018
[2] Estrategia europea de datos: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es

dentro de los espacios de datos sectoriales y la creación de entornos de tratamiento (p.ej., salas de datos), supervisados por el sector público. Otras iniciativas legislativas se centran en sectores específicos, como la Propuesta de espacio de datos sanitarios de la UE [7]. Para el sector privado, la Propuesta de Ley de Datos de la UE [8], pretende establecer las normas para crear nuevo valor a partir de los datos que poseen los consumidores y empresas, y aclarar quién puede acceder a esos datos y en qué condiciones. A través de la Ley de Datos de la UE, las empresas, los ciudadanos y las administraciones públicas podrán compartir datos sobre la base de medidas específicas destinadas a aumentar la seguridad jurídica, evitar el abuso de los desequilibrios contractuales y facilitar el acceso a los datos a los organismos del sector público.

1.2 EL PAPEL DE LA INGENIERÍA DE PROTECCIÓN DE DATOS

La ingeniería de protección de datos puede ser un factor clave para construir un entorno compartido de confianza con un nivel de protección adecuado.

La protección de los datos personales es un elemento integral de la confianza que los particulares y las organizaciones deben tener implementado en el desarrollo de ecosistemas de compartición de datos. Como se destaca en el dictamen conjunto del CEPD y la SEPD [9], el éxito dependerá también del *establecimiento de una gobernanza de datos sólida y de salvaguardias eficaces de los derechos e intereses de las personas físicas que sean plenamente conformes con el RGPD*. Aquí es donde la ingeniería de protección de datos tiene un papel muy importante que desempeñar. Las iniciativas legislativas que promueven la compartición de datos son instrumentos sectoriales e intersectoriales que tienen como objetivo hacer que los datos estén disponibles mediante la regulación de la reutilización de datos de titularidad pública y privada, incluidos los datos personales. También facilitan el intercambio de datos mediante la creación de intermediarios y entornos de intercambio novedosos en los que las partes implicadas pueden compartir datos e instalaciones de forma fiable y segura.

La ingeniería de protección de datos, tal y como se describe en [10], puede ser un factor clave para construir un entorno de compartición de confianza, en el que las organizaciones puedan presentar datos sin revelar datos personales o información empresarial sensible o revelando datos personales con un nivel de protección adecuado. Esto se ajusta al espíritu del concepto de protección de datos por diseño prescrito en el art. 25 del RGPD; las salvaguardias deben integrarse y diseñarse en el tratamiento. La ingeniería de protección de datos ofrece la posibilidad de hacer frente a las crecientes capacidades de las tecnologías de transmisión, almacenamiento y tratamiento sin disminuir su potencial de innovación y, al mismo tiempo, mitigar los riesgos emergentes para la privacidad de las personas y los riesgos económicos para las empresas.

Como ha señalado el Comité Europeo de Protección de Datos (CEPD) en sus directrices sobre protección de datos desde el diseño y por defecto [11] en un mundo cada vez más digital, la adhesión a la protección de datos desde el diseño desempeña un papel crucial en la promoción de la privacidad y la protección de datos. Es crucial que los titulares de los datos comprendan los principios de la protección de datos y los derechos y libertades de los interesados, e implementen las medidas adecuadas y las salvaguardias necesarias para reforzar estos principios y permitir el ejercicio de estos derechos. Cada medida técnica y organizativa debe producir los resultados previstos en el contexto específico en el que tiene lugar el tratamiento.

Por lo tanto, es necesario prestar especial atención a la identificación de los principales paradigmas de ingeniería de protección de datos en el intercambio de datos y a la comprensión de los tipos de salvaguardias que deben implementarse en todos los escenarios posibles. En los siguientes capítulos de este documento se ejemplificarán con más detalle estos paradigmas y las salvaguardias técnicas pertinentes a través de casos de uso prácticos. Estos casos de uso se centran principalmente en el sector sanitario; no obstante, las tecnologías y técnicas presentadas son igualmente aplicables a otros ámbitos de aplicación.

1.3 CAMPO DE ACCIÓN Y OBJETIVOS

Este informe pretende analizar con detalle casos de uso específicos relacionados con la compartición de datos personales, principalmente en el sector sanitario, y analiza cómo las tecnologías específicas y las consideraciones de implementación pueden apoyar el cumplimiento de los principios específicos de protección de datos. Tras analizar algunos de los retos de la compartición de datos (personales), este informe muestra cómo diseñar tecnologías y técnicas específicas que permitan compartir datos y preservar la privacidad. Este trabajo está pensado para apoyar a los responsables de las políticas, los reguladores y los profesionales de la protección de datos y se lleva a cabo en el contexto de las tareas de ENISA en virtud del Reglamento sobre la Ciberseguridad (CSA, por sus siglas en inglés)[3] para apoyar a los Estados miembros en aspectos específicos de ciberseguridad de la política y la legislación de la Unión en relación con la protección de datos y la privacidad. Este trabajo se basa en las actividades de la Agencia en el ámbito de la Ingeniería de Protección de Datos [10] y se realiza en colaboración con el Grupo de Trabajo Ad Hoc de ENISA sobre Ingeniería de Protección de Datos[4].

1.4 ESTRUCTURA DEL DOCUMENTO

La sección 2 analiza casos concretos de uso de compartición de datos en el sector sanitario, con el objetivo de mostrar cómo pueden cumplirse los principios de protección de datos mediante el uso adecuado de soluciones tecnológicas basadas en técnicas criptográficas avanzadas. La sección 3 aborda la compartición de datos que tiene lugar como parte de otro proceso o servicio, en el que los datos se procesan mediante un canal o entidad secundarios antes de llegar a su destinatario principal. Por último, la sección 4 analiza los retos, consideraciones y las posibles soluciones arquitectónicas sobre aspectos de control por parte del interesado (como el derecho de supresión y el derecho de rectificación cuando se comparten datos). La sección 5 cierra el documento.

[3] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relative a ENISA (Agencia de Ciberseguridad de la Unión Europea) y a la certificación de la ciberseguridad de las tecnologías de la información y las comunicaciones y por el que se deroga el Reglamento (UE) N.º 526/2013 (Ley de Ciberseguridad)
http://data.europa.eu/eli/reg/2019/881/oj
[4] https://www.enisa.europa.eu/topics/data-protection/ad-hoc-working-group-on-data-protection-engineering

2. PRÁCTICAS DE COMPARTICIÓN DE DATOS EN EL SECTOR SANITARIO

Un ámbito en el que la compartición de datos supone una oportunidad es, sin duda, el sector sanitario. La compartición de datos sanitarios puede reforzar la coordinación y la colaboración entre las entidades sanitarias públicas y privadas para prestar una asistencia sanitaria personalizada eficaz y alcanzar los objetivos de salud pública, así como para llevar a cabo investigaciones científicas (incluidos ensayos clínicos) [12]. La compartición de datos en el sector sanitario también tiene dimensiones transfronterizas, como se señala en la Directiva sobre Asistencia Sanitaria Transfronteriza y actualmente en la propuesta de Espacios de Datos Sanitarios de la UE [7]. Sin embargo, existen varios riesgos para la protección de los datos personales que se derivan del carácter sensible de los datos sanitarios con arreglo al art. 9[5] del RGPD y del hecho de que, para garantizar el cumplimiento de principios de protección de datos como la transparencia y la minimización de datos, se requiere una evaluación muy exhaustiva y un planteamiento prudente de implementación “desde el diseño” [12].

Un planteamiento básico para garantizar la transparencia del usuario es permitirle controlar quién tendrá acceso a sus datos, así como durante cuánto tiempo y a qué parte de sus datos.

Los datos sanitarios incluyen datos biomédicos, historiales médicos electrónicos (p.ej., historiales médicos almacenados y procesados en un hospital), y datos generados por las propias personas, p.ej. datos de dispositivos portátiles [14]. En el contexto de la compartición de datos sanitarios para diversos fines, es necesario abordar de manera eficiente las siguientes propiedades o requisitos [15].

- Los datos para el diagnóstico y tratamiento de pacientes individuales deben ser identificables.
- Los (mismos) datos para la investigación médica (posiblemente a gran escala) deben estar debidamente seudonimizados, a fin de garantizar que no sea probable que un investigador vuelva a identificarlos (a menos que el usuario dé su consentimiento explícito para el tratamiento sin seudonimizar, que puede ser revocable en cualquier momento)[6], así como existencia de la capacidad de eliminar el vínculo [16] entre dos conjuntos de datos diferentes para fines distintos.
- Debe existir la capacidad de gestionar múltiples fuentes de datos de pacientes, incluidos los dispositivos portátiles y las aplicaciones.

Cabe destacar que la necesidad de minimizar los datos abarca estos tres requisitos horizontalmente.

Otros requisitos de protección de datos que también deben cumplirse son la transparencia para el interesado y la seguridad de los datos.

2.1 COMPARTICIÓN DE DATOS PERSONALES CONTROLADOS POR EL USUARIO

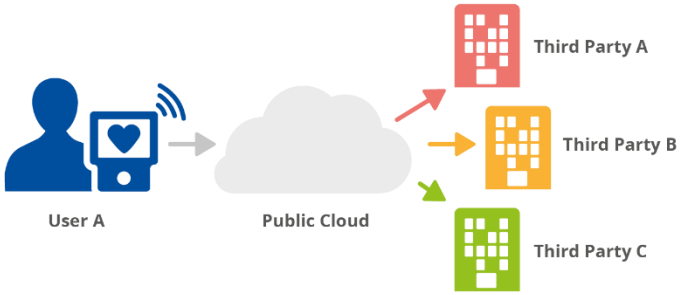
Un enfoque básico para garantizar la transparencia al usuario consiste en permitirle controlar quién tendrá acceso a sus datos, así como durante cuánto tiempo y a qué parte de sus datos.

[5] Según el RGPD, los datos sobre la salud no solo pertenecen a las denominadas “categorías especiales” de datos (art. 9), sino que los estados miembros tienen margen para introducir, en sus legislaciones nacionales, otras condiciones y limitaciones (aparte de las previstas en el RGPD) con respecto al tratamiento de estos datos, lo que ilustra claramente la importancia de su tratamiento.
[6] Desde un punto de vista jurídico, la base legal para dicho tratamiento es el consentimiento del usuario.

Por lo tanto, en este enfoque de compartición de datos controlado por el usuario, el papel de éste podría considerarse una "salvaguardia" para garantizar el cumplimiento de los requisitos de protección de datos antes mencionados. Desde el punto de vista de la base jurídica para el tratamiento, este enfoque es una manera de **implementar la compartición de datos con el consentimiento explícito del usuario de una manera que no puede ser superada**; no se permitiría a ninguna entidad acceder a los datos sanitarios del usuario a menos que éste concediera explícitamente el acceso.

Consideremos un escenario en el que el Usuario A utiliza un dispositivo portátil para la monitorización continua de la glucosa (CGM, por sus siglas en inglés), que también controla la presión arterial, los niveles de cafeína y los niveles de lactato[7]. El dispositivo carga los flujos de datos recogidos en la nube para su almacenamiento y posterior procesamiento para el propia usuario o para otras entidades, por ejemplo, su familia, médicos etc. como se muestra en la Figura 1 a continuación. El principal reto, desde el punto de vista de la protección de datos, es cómo el usuario puede compartir de manera selectiva flujos de datos específicos generados por el dispositivo con partes específicas.

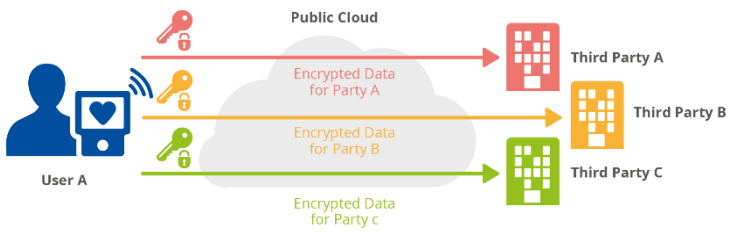
Figura 1: Modelo genérico de compartición de datos personales controlados por el usuario



Este modelo de acceso puede basarse no solo en la identidad de la entidad que solicita el acceso, sino también en parámetros adicionales como el periodo de tiempo en el que se generan los datos. Por ejemplo, podría concederse a un tercero acceso únicamente a los datos correspondientes a los tres últimos meses y/o a partes específicas del conjunto de datos (p.ej. mediciones de la presión sanguínea).

Un enfoque sencillo para alcanzar los objetivos es el uso de la codificación asimétrica. El Usuario A encripta los datos con la clave pública del destinatario correspondiente y comparte los datos tal y como se presenta en la Figura 2 a continuación. En otras palabras, cada segmento de datos que vaya a ser leído por un tercero se encripta con la clave pública de A (del mismo modo, si la propia usuaria va a acceder a los datos, se encriptan con la clave pública de la usuaria).

Figura 2: Compartición de datos controlado por el usuario mediante codificación asimétrica



[7] Aparentemente, nuestro escenario del caso de uso podría adaptarse fácilmente para describir el caso en el que el paciente utiliza más de un dispositivo portátil, cada uno con una finalidad diferente (p.ej. MGC, monitorización holter, etc.)

No obstante, este enfoque tiene algunas limitaciones, principalmente en términos de practicidad y eficiencia. Si los mismos datos deben compartirse con múltiples entidades, el usuario necesita compartir los mismos datos muchas veces, cada una de ellas cifrada con la clave pública de la entidad pertinente. Esto conduce inevitablemente a la redundancia, que se convierte en un problema predominante especialmente en el caso de grandes volúmenes de datos que se producen constantemente. Además, los posibles destinatarios no necesariamente se conocen de antemano y, en consecuencia, para cada nuevo acceso que se quiera conceder, sería necesaria una nueva codificación.

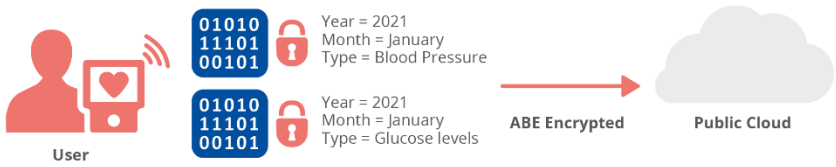
2.1.1 Codificación basada en atributos

Una técnica criptográfica para superar las limitaciones mencionadas es la Criptografía Basada en Atributos (ABE, por sus siglas en inglés)[8], que se introdujo por primera vez en 2004 con el término de cifrado Basado en Identidad Difusa [17] y [18]. ABE es un caso especial de codificación asimétrica, en el que los datos pueden cifrarse con una clave pública ABE, pero, a la vez, contrariamente a la codificación de clave pública "clásica", puede haber más de una clave de descifrado, cada una de ellas vinculada a pequeñas piezas de información adicional relacionada con los datos, que se denominan atributos. En realidad, las claves de descifrado se generan mediante una clave maestra secreta ABE genérica, que debe permanecer privada.

ABE es un tipo especial de cifrado asimétrico, en el que los datos pueden cifrarse con una clave pública ABE, pero puede haber más de una clave de descifrado.

Revisando el caso de uso analizado anteriormente, a continuación, describimos cómo se puede utilizar ABE para implementar la compartición de datos controlada por el usuario mediante un servicio en la nube. Nuestro escenario se basa en gran medida en la implementación descrita en [19]. No obstante, cabe señalar que hoy en día las infraestructuras y servicios en la nube ofrecen una amplia gama de posibilidades y pueden llevar a cabo parte de las operaciones de tratamiento, además de la transmisión de los datos. No obstante, estas aplicaciones quedan fuera del ámbito de los casos de uso descritos en este informe.

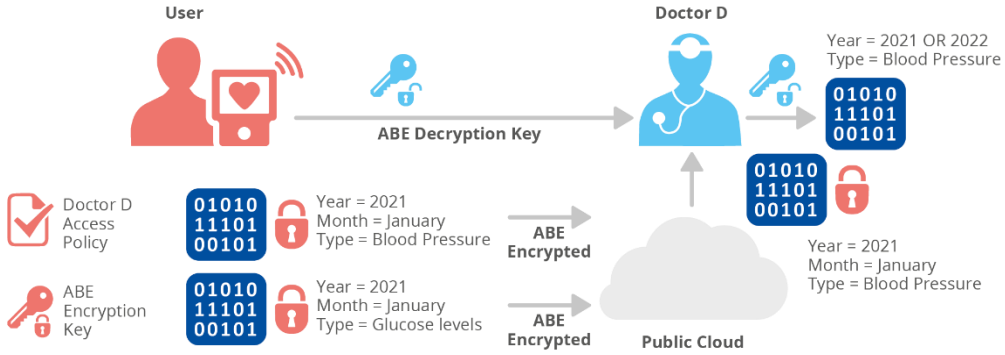
Figura 3: Almacenamientos de objetos codificados en la nube



Los datos del usuario son generados por su dispositivo y se asignan a objetos relevantes, describiendo atributos específicos relacionados con ellos, como la fecha de origen, el tipo de objeto, etc. Estos atributos se utilizarán posteriormente para definir el mecanismo de control de acceso a estos datos. A continuación, los datos se cifran con la clave maestra ABE y se suben a la nube.

[8] ABE puede considerarse como un caso específico del llamado cifrado funcional, que se define como un tipo específico de cifrado de clave pública que permite claves de descifrado con la propiedad de que solo pueden descifrar una función específica del texto sin formato cifrado (independientemente del contenido del texto sin formato).

Figura 4: Compartir la clave de descifrado ABE y los datos cifrados



Cuando un tercero solicita acceso a los datos de un usuario, el usuario A crea una política de acceso para ese tercero. Esta política especifica qué propiedades exactas, basadas en los atributos ya definidos, deben cumplir los datos a los que quiere conceder acceso. A continuación, el dispositivo del usuario "traduce" la política, por ejemplo archivo="presión arterial" y año>=2021 AND receptor="Doctor D", en una clave de descifrado ABE correspondiente, y envía la clave a la otra parte (el proveedor de la nube no tiene acceso a esta clave de descifrado). **Una vez que el doctor D reciba esta clave de descifrado, solo podrá descifrar localmente los datos correspondientes que satisfagan la política de acceso definida por el usuario, ya que la clave de descifrado ABE solo puede descifrar un subconjunto del conjunto de datos.**

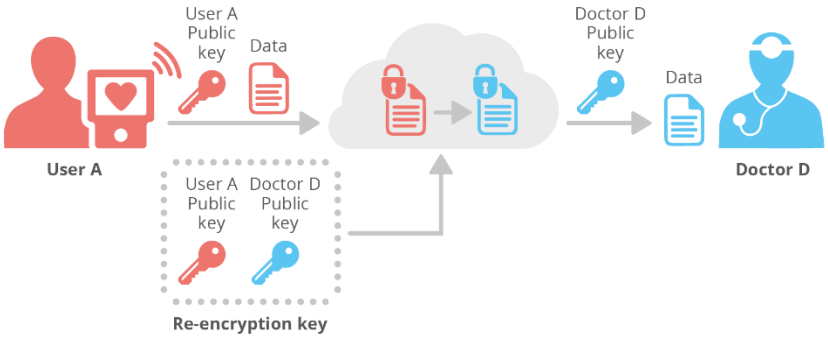
Sin embargo, este planteamiento permite "etiquetar" los datos en una fase temprana, lo que no siempre es una tarea sencilla, ya sea debido a las capacidades del dispositivo o a la interacción requerida por el usuario. Además, una selección adecuada de atributos en relación a las políticas de acceso posteriores puede no ser siempre obvia. Sin embargo, en un modelo de intercambio de datos controlado por el usuario, es inevitable que éste pueda tomar decisiones sobre sus datos. Además, el proveedor de la nube continúa recopilando información relacionada con los metadatos de cada comunicación entre el usuario y cada una de las partes.

2.1.2 Recodificación proxy

Otra tecnología criptográfica avanzada que permite la compartición de datos controlada por el usuario es la Recodificación proxy (PRE, por sus siglas en inglés) [20]. Se trata de un tipo específico de codificación asimétrico, que **permite volver a codificar un conjunto de datos ya codificados de una clave pública a otra,** sin que el proxy tenga acceso al conjunto de datos sin cifrar. Se considera un enfoque muy bueno cuando la entidad con la que se van a compartir los datos no se conoce en el momento de la codificación inicial o la compartición se va a llevar a cabo a través de infraestructuras no fiables.

Profundizando en el caso de uso descrito anteriormente, el Usuario A cifra sus datos con su propia clave pública y los sube a la nube. Cuando un tercero, por ejemplo, el Doctor D, solicita acceso a los datos, el usuario genera una clave de recodificación, utilizando su propia clave privada y la clave pública del doctor D. La clave de recodificación puede enviarse al proveedor de la nube, que ahora puede transformar el conjunto de datos cifrados correspondiente al cifrado mediante la clave pública del Doctor D, como se presenta en la Figura 5 a continuación. De este modo, **solo el Doctor D puede descifrar los datos utilizando su clave privada**.

Figura 5: Proceso de recodificación proxy



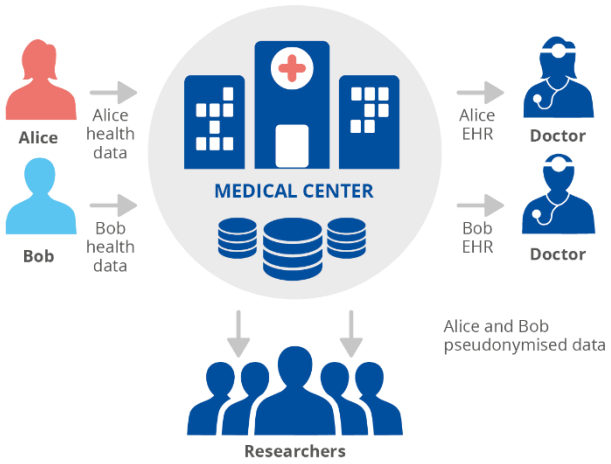
PRE permite un control de acceso reforzado criptográficamente en un modelo de compartición controlada por el usuario. Además, permite al propietario de datos delegar el acceso una vez cifrados, lo que es importante porque en un escenario típico de compartición no siempre es posible identificar de antemano a las entidades destinatarias.

En general, PRE puede considerarse una buena solución cuando el intercambio se realiza a través de infraestructuras no fiables, como una infraestructura en la nube. En [21] ya se describen varias aplicaciones y patentes comerciales existentes. Sin embargo, el proveedor de la nube sigue recopilando información relacionada con los metadatos de cada comunicación, de forma similar al ABE comentado anteriormente. Además, como la recodificación solo puede llevarse a cabo sobre el conjunto de datos inicialmente cifrados, el usuario debe tener un buen conocimiento durante la codificación inicial de los datos que serían compartidos posteriormente. Cabe destacar, no obstante, que ABE y PRE pueden usarse de forma combinada [22], lo que permite una compartición de datos controlada por el usuario de una manera más fina.

2.2 INTERCAMBIO DE DATOS SANITARIOS CON FINES MÉDICOS Y DE INVESTIGACIÓN POR PARTE DE LOS PROVEEDORES DE ASISTENCIA SANITARIA

Otro escenario típico de intercambio de datos en el sector sanitario es la gestión de Historias Clínicas Electrónicas (HCE) por parte de los proveedores de asistencia sanitaria. A grandes rasgos, las HCE son una versión electrónica del historial médico de un paciente que contiene todos los datos médicos clave relativos a las afecciones de esa persona, los resultados de exámenes médicos, tratamientos, medicamentos etc. Las HCE suelen gestionarse con un repositorio central a nivel nacional y los usuarios pueden autorizar el acceso a sus datos a médicos tratantes o a las instituciones médicas. Durante la pandemia, la necesidad de proyectos de recopilación de datos a gran escala se hizo aún más patente, en un intento de apoyar no solo el tratamiento de los pacientes, sino también la investigación científica y el pronóstico.

Figura 6: Ejemplo de recopilación de datos a gran escala



Mediante la codificación polimórfica, los datos pueden cifrarse de tal manera que no es necesario fijar a priori quién puede descifrarlos.

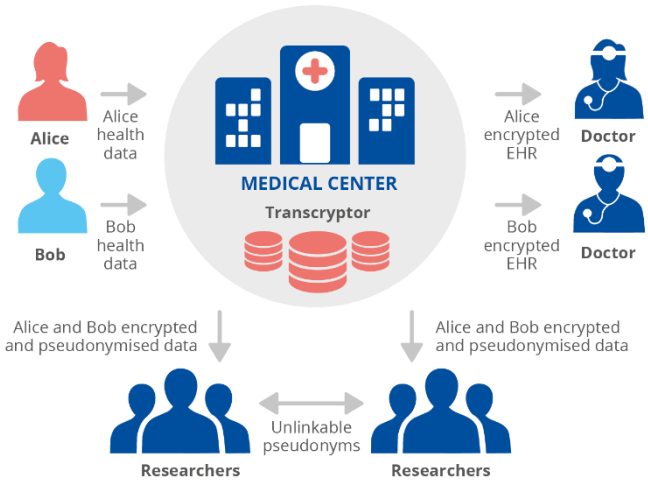
Normalmente, para abordar las cuestiones de protección de datos que les son de aplicación, un centro médico despliega mecanismos de control de acceso, aplicables tanto a usuarios internos como externos, para determinar quién tendrá acceso a los datos y/o la codificación de los datos almacenados. **El objetivo es garantizar que solo los proveedores de servicios sanitarios autorizados tendrán acceso a la información personalizada** (por ejemplo, médicos que necesiten acceder al historial médico de un paciente). **Cuando los datos deben compartirse con investigadores internos o externos con fines de investigación, deberán desplegarse además las salvaguardias adecuadas que, en un escenario típico, incluyen la seudonimización para evitar la revelación de la identidad de los pacientes a los destinatarios**, tal y como se describe en [12] y se presenta en la Figura 6 anterior.

2.2.1 Codificación polimórfica y seudonimización

Aprovechando las ventajas de la codificación polimórfica, se propuso la Codificación Polimórfica y Seudonimización (PEP, por sus siglas en inglés) [15] como medio para hacer frente a los retos descritos anteriormente. La principal propiedad de la codificación polimórfica es que los datos personales pueden cifrarse de tal manera que no es necesario fijar a priori quién puede descifrarlos. Esto puede decidirse más tarde mediante transformaciones del texto cifrado que permitan llevar a cabo el descifrado a través de diferentes claves criptográficas. Esta transformación puede realizarse de forma ciega sin que la parte que la lleva a cabo, el transcriptor, pueda acceder al conjunto de datos sin cifrar. Por lo tanto, el transcriptor "transforma" el conjunto de datos encriptados en otra versión que solo el destinatario puede descifrar [15]. El transcriptor puede ser una entidad dentro de la organización (por ejemplo, el centro médico o el hospital) o de fuera de la organización, por ejemplo, un proveedor de la nube. Con respecto a la seudonimización, PEP utiliza el transcriptor también como entidad de seudonimización, como se describe en [23]. A cada individuo se le asignan seudónimos diferentes para cada tercero que solicite acceso a sus datos, evitando así la vinculación de seudónimos entre múltiples terceros.

Volviendo al caso de uso de los proyectos de recopilación de datos a gran escala en el sector sanitario comentado anteriormente, cada paciente tiene un identificador único. **El transcriptor transforma este identificador en varios seudónimos dependiendo del destinatario y del contexto o propósito de compartir los datos. Cada seudónimo se comunica a cada destinatario junto con los datos cifrados polimórficos**. Como para cada destinatario se genera un nuevo seudónimo, los seudónimos utilizados para el mismo paciente no pueden vincularse, por lo que se consideran no vinculables y preservan la confidencialidad de los datos del paciente. Como se muestra en la Figura 7, cuando el destinatario es un médico, el transcriptor vuelve a cifrar los datos sanitarios del paciente y los transmite al médico correspondiente.

Figura 7: Utilizar la PEP en una recopilación de datos a gran escala



Debe tenerse en cuenta que el tratamiento de datos seudónimos siempre está sujeto a la reidentificación de los individuos, ya sea mediane la reversión de los seudónimos a los identificadores originales o mediante la reidentificación de los individuos a través de la información personal restante que queda disponible (los denominados cuasi-identificadores) como se discute en [23]. En general, la PEP constituye una técnica que actualmente se considera una técnica criptográfica avanzada para la ingeniería de protección de datos y que ya ha demostrado su aplicabilidad en un estudio a gran escala de la enfermedad de Parkinson [24] y como propuesta para el plan holandés de identificación electrónica [25].

3. COMPARTICIÓN DE DATOS MEDIANTE SERVICIOS DE TERCEROS

Además de los casos de uso de compartición de datos, en los que una entidad comparte datos directamente con otra entidad, que es el destinatario final de los datos, también existen casos de compartición de datos secundarios, no directos, que también pueden requerir que un usuario lleve a cabo acciones específicas. En este tipo de compartición de datos, **la compartición tiene lugar como parte de otro proceso o servicio, en el que los datos se procesan a través de algún canal o entidad secundarios antes de llegar a su destinatario principal**. A menudo, esta compartición de datos no es transparente a los usuarios. De ahí que este tema deba ser abordado por ingenieros, arquitectos y desarrolladores especializados en privacidad. Por ejemplo, esta compartición de datos se produce cuando una aplicación integra un servicio de tercero, que también está gestionado por una entidad distinta del destinatario o remitente principal de los datos [26]. Aunque se trata de una práctica establecida en el desarrollo de *software*, hay casos en los que esto es perjudicial para la privacidad de los usuarios, p.ej. un componente o un servicio utilizado puede compartir datos con un tercero – a veces, sin que los arquitectos y los desarrolladores del sistema lo sepan.

Existen ejemplos de casos de uso de compartición de datos secundarios en muchas dimensiones de la ingeniería de *software*. La tabla 1 ofrece una visión general de algunos de estos casos de uso estructurados en tres ámbitos principales, así como una descripción de alto nivel de cada uno de ellos.

Tabla 1: Casos de uso seleccionados de compartición de datos de terceros

Ámbito	Caso de uso	Descripción
Integración de servicios de terceros	Notificaciones *push* para móviles	Utilización de un servicio de terceros para enviar notificaciones *push* a usuarios de teléfono móvil (apps)
	Autenticación y autorización	Integración de un servicio de autenticación y/o autorización de terceros en una aplicación, p.ej. identidad federada.
Externalización de las operaciones informáticas	Supervisión de la red	Siempre que se lleva a cabo una supervisión de la red, especialmente por parte de una empresa subcontratada, se produce una compartición implícita de datos.
	Compartición de datos entre el entorno local y la nube	Cuando las empresas implementan un enfoque de nube hibrida, los datos se comparten entre el entorno local y la nube.
Optimización de preparación de hilos	Compartir información de inteligencia	Esfuerzos de colaboración para compartir información oportuna y adecuada sobre amenazas emergentes dentro de una comunidad predefinida.

En el marco de este estudio, no centramos en los dos primeros casos de uso, a saber, las notificaciones *push* para móviles y la autenticación, que se analizarán con más detalle.

3.1 NOTIFICACIONES PUSH PARA MÓVILES

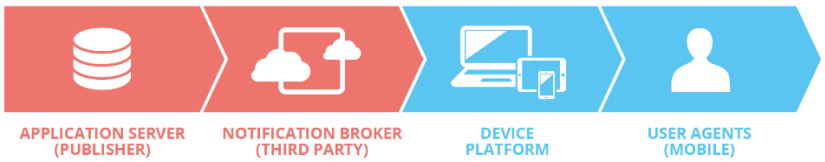
Las notificaciones *push* para móviles son un importante canal de comunicación entre las aplicaciones móviles y sus usuarios. Mediante los mensajes *push*, un proveedor de aplicaciones móviles puede enviar instantáneamente un mensaje a sus usuarios. Las notificaciones *push* pueden proporcionar información oportuna del proveedor de la aplicación al usuario o usuarios y, potencialmente, provocar una reacción por parte de estos últimos.

Las notificaciones *push* para móviles pueden transmitir diferentes tipos de contenido, como texto, imágenes, enlaces externos y dentro de la aplicación, etc. Además de con fines de *marketing*, las notificaciones *push* también pueden utilizarse para provocar una reacción por parte del usuario o usuarios, o para indicar a los usuarios que proporcionen una determinada información, que lleven a cabo un determinado proceso que ofrezcan una funcionalidad. De ahí que la puntualidad de la notificación *push* sea a menudo importante y, generalmente, su principal ventaja frente a otros canales de comunicación, como el correo electrónico o los mensajes de texto. Los mensajes *push* para móviles pueden mandarse en masa o individualmente (personalizados).

En el caso de las notificaciones personalizadas, la información transmitida puede muy bien incluir datos personales o seudónimos como identificadores de aplicaciones de usuario. De ahí que sea necesario integrar medidas técnicas y organizativas adicionales para hacer frente a las amenazas a la privacidad que se describen a continuación. Actualmente, una de las plataformas más utilizadas para las notificaciones *push* es la mensajería multiplataforma *Firebase Cloud Messaging* (FCM),[9] compatible con los dos principales sistemas operativos móviles (iOS y Android).

Desde el punto de vista de la ingeniería, los desarrolladores suelen integrar código proporcionado por terceros en su aplicación. Aunque puede no ser transparente para los usuarios, la infraestructura de las notificaciones *push* para móviles implica, al menos, dos entidades adicionales, que son fundamentales para su arquitectura en el mundo móvil. Así, tenemos las siguientes entidades, que se representan en la Figura 8 y se describen a continuación.

Figura 8: Principales actores de las notificaciones *push* para móviles



- **Servidor de aplicaciones (Editores):** servidor de aplicaciones típico, que envía un mensaje de notificación al usuario de una aplicación móvil;
- **Notificación Broker (Tercero):** un tercero que proporciona intermediación de notificaciones *push* a los usuarios finales (agentes de usuario);
- **Plataforma del dispositivo / SO:** el contacto del broker de notificaciones con la aplicación debe realizarse a través de una API dedicada proporcionada por el sistema operativo del dispositivo, como Android, iOS, etc; se contacta con la plataforma del dispositivo / SO independientemente de la participación del agente de notificaciones;

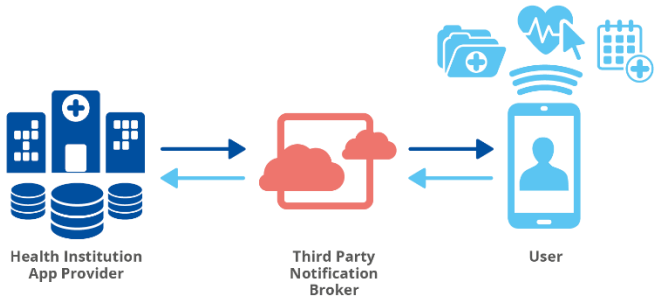
[9] Mensajería en la nube Firebase (FCM, por sus siglas en inglés): https://firebase.google.com/docs/cloud-messaging

- **Agente de usuario (Móvil):** suele estar representado por una aplicación móvil, que se ejecuta en la plataforma del dispositivo correspondiente y representa la interfaz de *software* interface para el usuario móvil.

Veamos el siguiente ejemplo de notificaciones *push* móviles en el ámbito de la salud. Una institución sanitaria ofrece una aplicación móvil que permite la interacción del usuario con los médicos, las instalaciones de la institución como los laboratorios y recepción y servicios personalizados para el usuario. El usuario puede recibir copias de los resultados de análisis de sangre, radiografías, resonancias magnéticas y recetas en la aplicación. También puede reservar citas con los médicos y recibir notificaciones de las próximas citas, recordatorios para reservar una revisión anual e incluso recordatorios diarios sobre la recepción de la medicación que le han recetado.

La aplicación móvil ofrece notificaciones *push* para todos los servicios mencionados. El usuario recibe recordatorios de próximas citas, exámenes anuales, meditación recibida y resultados de laboratorio en cuanto están disponibles, y puede responder o devolver información a la institución sanitaria interactuando con la notificación *push*.

Figura 9: Entidades implicadas en el escenario de las notificaciones push móviles de e-Salud



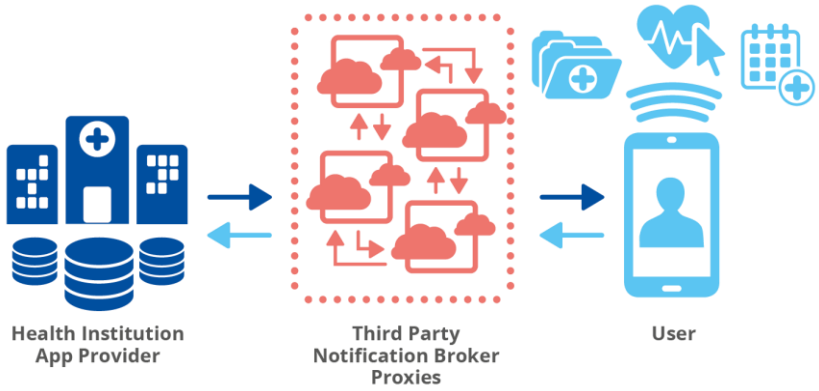
El tercero que opera el servicio de intermediación de notificaciones recibe los datos de las notificaciones del servidor de aplicaciones y los entrega al cliente agente usuario. Por lo tanto, se comparten datos indirectamente con un tercero, lo que plantea amenazas a la privacidad del usuario, entre otras:

- **Vinculabilidad (*linkability*)**: observación de la interacción entre las dos entidades, incluida la frecuencia de la interacción, los tipos de mensajes intercambiados, etc.;
- **Identificabilidad**: mensajes que identifican al usuario;
- **Divulgación**: el contenido de los mensajes que se envían puede ser divulgado, violando así la confidencialidad de la notificación, ya que en muchos casos estos mensajes se envían a través del tercero en claro.

3.1.1 Protocolos de notificación anónima (mediante Proxies)

Un enfoque para hacer frente a las amenazas a la privacidad mencionadas anteriormente podría llevarse a cabo mediante el uso de protocolos de notificación privados, que permiten la entrega de mensajes de notificación mediante el uso de múltiples capas de anonimización o proxies, como se describen también en [10]. Este enfoque requiere el uso de una cadena de proxies, a través de la cual los mensajes de notificación podrían mezclarse antes de llegar al usuario final. este tipo de protocolos permite enviar servicios de notificaciones *push* móviles a los usuarios sin que los nodos intermediarios conozcan ni al remitente original ni al destinatario final.

Figura 10: Visión general de la arquitectura de proxies



Basándose en el ejemplo descrito anteriormente, un mensaje de notificación en este enfoque se enviaría a través de una cadena de proxies. El proveedor de la aplicación prepararía el mensaje y escogería una selección aleatoria de nodos intermediarios (proxies), a través de los cuales se enrutaría el mensaje. En este caso, no existe uno sino una mezcla de servidores de intermediación de notificaciones. Cada uno de ellos solo conoce la dirección del siguiente servidor de intermediación, ocultando la información sobre las dos entidades finales (servidor de aplicaciones y usuario). Además, la propia comunicación entre los servidores de notificación (proxies) se cifra con sus correspondientes claves públicas, protegiéndose así de una divulgación involuntaria. Un ejemplo de este tipo de protocolo es AnNotify [27], que admite la desvinculación de la notificación entre el subscriptor y el editor, la desvinculación de las notificaciones *push* a un subscriptor y la privacidad de la difusión, ocultando si un subscriptor está suscrito o no a una notificación.

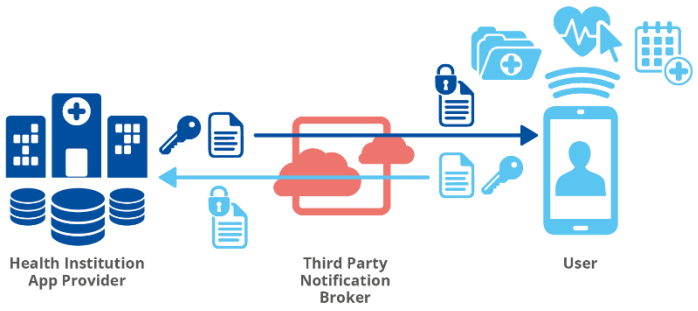
Independientemente del protocolo elegido, es necesario tener en cuenta las implicaciones potenciales tanto para el desarrollo como para el funcionamiento del servicio que utilice dicho protocolo, con el fin de proporcionar viabilidad práctica y ser adoptado por los desarrolladores. A este respecto, pueden utilizarse varios criterios para evaluar las distintas opciones, como la facilidad de integración en la aplicación, la facilidad de mantenimiento, la escalabilidad, etc.

3.1.2 Cifrado de extremo a extremo

El cifrado de los mensajes de notificación es la medida más directa para hacer frente al menos a algunas de las amenazas de privacidad mencionadas anteriormente (sobre todo la de divulgación). En la actualidad, la entrega de notificaciones *push* no suele llevarse a cabo mediante cifrado de extremo a extremo. O bien no se utiliza codificación alguna, o solo se cifra una parte de la comunicación. En algunos casos, el desarrollador, o desarrolladores, puede decidir entregar el mensaje de notificación entre el servidor de aplicaciones y el agente de notificaciones utilizando el cifrado en la capa de transporte (p.ej. TLS), que proporciona cifrado entre estas dos entidades. Además, un agente de notificaciones puede optar por cifrar la comunicación con el usuario (dispositivo). Sin embargo, la codificación es parcial y no aborda plenamente la amenaza de divulgación a través de cada una de estas entidades. El agente de notificaciones descifra el mensaje antes de enviarlo al usuario. Una solución más adecuada para esto sería la implementación de un cifrado de extremo a extremo como mínimo.

Los detalles de este enfoque se muestran a continuación en la Figura 11. El proveedor de aplicaciones utiliza la clave pública del usuario y codifica el contenido del mensaje que se envía. Aunque el servidor de aplicaciones sigue utilizando el agente de notificaciones para enviar el mensaje, no puede descifrarlo. Simplemente entrega los mensajes de notificación sin poder leer el mensaje enviado. A continuación, al recibir el mensaje de notificación en su teléfono, el usuario puede utilizar su clave privada para descifrarlo y leer el mensaje enviado.

Figura 11: Cifrado de extremo a extremo



Con este enfoque, el agente de notificaciones no tiene acceso al contenido de la notificación. No obstante, podría observar los metadatos y conocer las interacciones entre las otras dos entidades. El Capillary Project[10], por ejemplo, pretende resolver este problema cifrando de extremo a extremo los mensajes de notificación, aunque se limita a aplicaciones Java en plataformas Android.

3.1.3 Estrategias de diseño

Además de las opciones técnicas descritas anteriormente, las decisiones sobre el diseño de la arquitectura que integran la privacidad desde el diseño podrían utilizarse para hacer frente a algunas de las amenazas comentadas anteriormente. Una de estas decisiones es, por ejemplo, seguir **una estrategia en dos pasos**. En el primer paso, la arquitectura debe exigir que se limite el uso de notificaciones *push* en la aplicación. Esto puede lograrse, por ejemplo, utilizando una estrategia "*pull by default*", por la que la funcionalidad de las notificaciones *push* se limita al mínimo y solo se utiliza para transferir datos no personales. En estos casos basta con notificar al usuario que existe una actualización o que se requiere una interacción. A continuación, en el siguiente paso, el mensaje de notificación, que incluye contenido personalizado, puede obtenerse directamente de la aplicación a través de una comunicación directa con el servidor de aplicaciones.

Siguiendo el ejemplo anterior, la aplicación electrónica de salud podría notificar al usuario que es necesario realizar una determinada acción o que hay un nuevo mensaje para él, pero sin mostrar el mensaje en sí. El usuario puede entonces reaccionar de forma proactiva haciendo clic en la aplicación. Sin embargo, está claro que esto es complementario a las otras medidas presentadas anteriormente, ya que puede reducir, por ejemplo, la amenaza de divulgación a terceros, pero no evitarla por completo. Además, este enfoque supone un reto, ya que requiere que se cubra todo el alcance de las funciones de notificación de una aplicación. Por lo tanto, se recomienda su uso como medida complementaria pero no principal, o cuando otras medidas no sean viables.

3.2 COMPARTICIÓN DE DATOS DURANTE LA AUTENTICACIÓN

La autenticación es un elemento clave para muchas aplicaciones web. Sin embargo, en algunos casos basta con obtener pruebas de que un interesado cumple con unos criterios específicos o tiene una propiedad concreta, en lugar de revelar todas las propiedades de su identidad y luego calcular si esas propiedades se cumplen o no.

La verificación de la edad ha sido uno de los métodos utilizados para garantizar la protección de los menores frente a posibles daños en el mundo físico; la tradicional verificación del DNI en las cajas de las tiendas es un buen ejemplo. En la actualidad, varias plataformas de compartición de vídeos exigen la verificación de la edad en virtud de lo dispuesto en la Directiva de servicios de comunicación audiovisual [28].Esta verificación acostumbra a llevarse

[10] https://github.com/google/capillary

a cabo mediante una autodeclaración de la fecha de nacimiento sin más validación. Aparte de la facilidad con la que se puede eludir este control, también está a cuestión del tratamiento de más datos de los necesarios para cumplir la finalidad especifica (principio de minimización de datos).

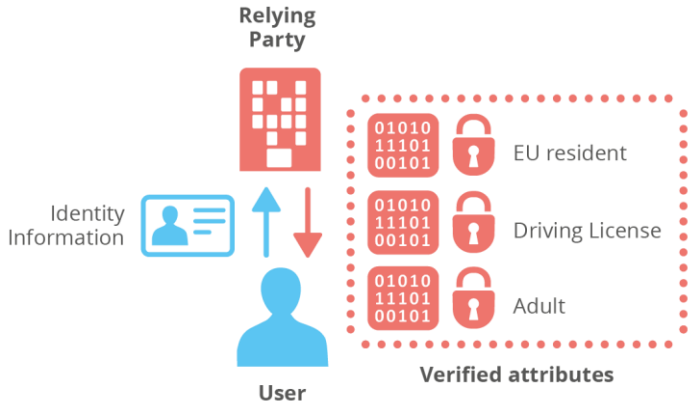
Los ABC con privacidad mejorada permiten autenticar una entidad revelando y autenticando selectivamente atributos específicos, sin revelar información adicional sobre la identidad.

Las Credenciales Basadas en Atributos (ABC, por sus iniciales en inglés) y, más concretamente, las ABC mejoradas en términos de privacidad permiten autenticar a una entidad revelando y autenticando selectivamente atributos específicos, sin revelar información adicional sobre la identidad que suele utilizarse e incluye datos personales [10]. El usuario presenta sus atributos a un tercero que verifica su exactitud y actúa después como tercero de confianza. Este enfoque ya ha demostrado su potencial y aplicabilidad en diferentes escenarios en el marco del proyecto de investigación *Attribute-based Credentials for Trust* (ABC4Trust) [29] e IRMA en el marco del proyecto *Future ID* [30].

Consideremos un servicio en línea de alquiler de coches dentro de la UE que ofrece un servicio de entrega. Durante el proceso de reserva en línea, se pide al usuario que presente información sobre si es mayor de 18 años y si tiene un permiso de conducir válido. Normalmente, esta información se verifica en el momento de recoger el vehículo alquilado y firmar el contrato de alquiler, pero con el servicio de entrega, el usuario puede firmar electrónicamente el contrato de alquiler. En lugar de demostrar por correo su edad y la validez de su permiso de conducir, el proveedor puede comprobar si se cumplen esos criterios validando atributos específicos de la identidad del usuario.

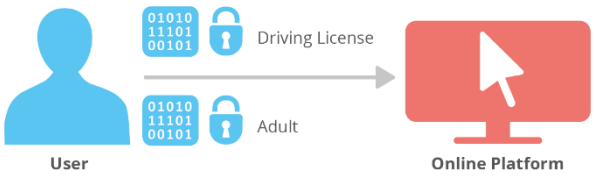
El usuario envía sus atributos a la entidad de confianza, que los valida y firma digitalmente. Ahora el usuario puede comunicarlos a terceros que puedan validar su autenticidad e integridad a través de la firma digital que los acompaña, como se presenta a continuación en la Figura 12.

Figura 12: Creación de atributos de identidad



Cuando el usuario visita el sitio web del servicio en línea de alquiler de coches, se le pide que proporcione los atributos pertinentes para demostrar que es mayor de 18 años y que posee un permiso de conducir válido. A continuación, el usuario presenta los atributos pertinentes a la plataforma en línea, ya sea mediante su tarjeta inteligente o a través de una extensión pertinente del navegador. La plataforma los valida y continúa con el proceso de reserva del coche de alquiler.

Figura 13: Autenticación basada en atributos



En este escenario de compartición de datos, **el usuario no revela los datos personales reales, sino un atributo que es un testimonio de un tercero de que se cumple (o no) una propiedad específica**.

3.2.1 Relevancia del acceso basado en atributos a las plataformas en línea

En 2022, la autoridad francesa de protección de datos (CNIL) destacó en [31] que no es posible aspirar a la eficacia absoluta del control de la edad en línea, especialmente en el caso de los menores. Dados los crecientes requisitos para la verificación de la edad de los menores en los servicios en línea, la CNIL recomienda el uso de un tercero independiente de confianza para promover la minimización de datos y la recopilación innecesaria de datos personales de los proveedores de servicios. La CNIL ofrece una visión general de seis posibles soluciones de verificación de edad existentes, pero concluye que ninguna de ellas cumple todas las propiedades requeridas en términos de fiabilidad, protección de datos y seguridad. Además de este análisis, el Laboratorio de Innovación Digital de la CNIL (LINC) ha desarrollado un sistema de verificación de la edad respetuoso con la privacidad[11] basado en la prueba de conocimiento cero.

La recomendación de la CNIL de un tercero de confianza y de **una autenticación basada en atributos, que se relaciona estrechamente con el concepto de prueba de conocimiento cero, parece un concepto bastante prometedor** para el Reglamento Servicios Digitales [32] Art. 28.2 disposiciones sobre la protección en línea de los menores. Según esta disposición, *los prestadores de plataformas en línea no presentarán anuncios en su interfaz basados en la elaboración de perfiles, tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679, mediante la utilización de datos personales del destinatario del servicio cuando sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor*.

Basándose en el caso de uso de terceros de confianza comentado anteriormente, el tutor o padre del menor podría apoyar la creación de una identidad basada en atributos para el menor que utilice dicho servicio de terceros. Entonces el menor podría navegar en plataformas en línea y hacer uso de las funcionalidades de la identidad basada en atributos, sin tener que revelar su identidad completa, fecha de nacimiento, etc. Este planteamiento satisfaría los requisitos de fiabilidad, protección de datos y seguridad de los datos del menor.

[11] https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process

4. CONSIDERACIONES SOBRE EL EJERCICIO DE LOS DERECHOS DE LOS INTERESADOS

Un elemento clave del RGPD es el derecho de los interesados a estar debidamente informados y a controlar el uso u otro tipo de tratamiento de los datos personales que les conciernan. Estos derechos de los interesados incluyen, entre otros, aspectos relacionados con los principios de protección de datos de licitud, equidad y transparencia (es decir, derecho de información y acceso), no vinculabilidad (es decir, minimización de datos, limitación de la finalidad y limitación del almacenamiento, integridad y confidencialidad) y control por parte del interesado (*intervenability*) (es decir, derecho de supresión, derecho de rectificación, derecho de oposición, así como a presentar reclamaciones ante las autoridades de protección de datos y a interponer recursos judiciales efectivos contra las autoridades de protección de datos; o los responsables o encargados del tratamiento).

Estos derechos fundamentales de los interesados exigen un examen más detenido en lo que respecta a su aplicación en entornos de compartición de datos. Mientras que las secciones anteriores cubren múltiples ejemplos de técnicas de minimización de datos, eliminando información de los datos o restringiendo el acceso a la información a un subconjunto más reducido de interesados, abordando así el objetivo de proteger la desvinculación, los otros dos objetivos de protección requieren un enfoque de ingeniería diferente. Este capítulo abordará estos aspectos.

A modo de ejemplo, hemos elegido el ámbito de aplicación de la asistencia sanitaria, tal y como se expone en la Sección 2. En este escenario, múltiples actores participan en la recogida de datos, su almacenamiento, intercambio y tratamiento. Los datos se crean en múltiples lugares, por ejemplo:

- en pacientes en hospitales o consultas médicas;
- en usuarios de dispositivos portátiles;
- en oficinas de empadronamiento o instituciones sanitarias gubernamentales;
- en compañías de seguros sanitarios;
- en fabricantes de dispositivos médicos;
- en guarderías o residencias de ancianos.

Cada una de estas fuentes de datos puede proporcionar datos de interés, como las condiciones médicas actuales y el historial médico, información estadística sobre edad, sexo, diagnósticos actuales y recientes de enfermedades, medicación en curso y pasada, hábitos y preferencias personales con respecto al deporte, la nutrición, el sueño, la vida familiar, etc. Aunque algunos Estados miembros europeos fomentan un enfoque centralizado del almacenamiento de datos sanitarios en instituciones alojadas por el gobierno, siempre habrá conjuntos de datos relevantes no almacenados en estos repositorios centrales. Por lo tanto, cuando se trata de la ingeniería de los derechos de los interesados, puede haber casos con un panorama muy segregado de responsables del tratamiento de datos, procesadores de datos y lugares de almacenamiento de datos.

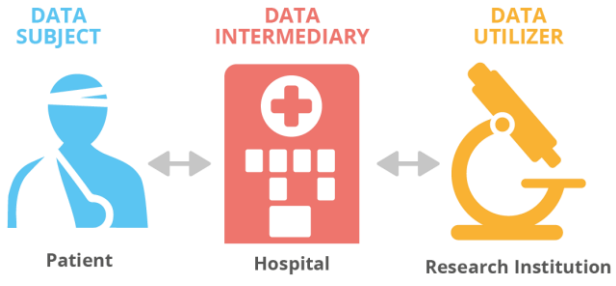
Como también se ha expuesto en la Sección 2, el RGPD contiene requisitos específicos relativos a los datos personales en el sector sanitario y proporciona un amplio conjunto de derechos del interesado. Dependiendo de las circunstancias exactas, esto puede afectar a los datos personales almacenados en hospitales, donde la finalidad vinculante, la declaración o retirada del consentimiento[12], las solicitudes de transparencia y los derechos de intervención deben considerarse adecuadamente.

En el otro extremo del debate sobre la compartición de datos, las organizaciones de tratamiento de datos están interesadas en adquirir datos para sus fines con suficiente apoyo técnico y directrices claras sobre las finalidades legítimas e ilegítimas de utilización de los datos. Para evitar confusiones con los términos del RGPD "responsable del tratamiento" y "encargado del tratamiento", y teniendo en cuenta que puede haber incluso una utilización basada en datos anónimos que no esté regulada por el RGPD, en este capítulo llamaremos a estas entidades "utilizadores de datos". En términos del RGPD, pueden ser responsables del tratamiento, encargados del tratamiento o destinatarios de los datos. Sin embargo, esto aún está por aclarar, dependiendo de cada escenario, como también se destaca en el Dictamen conjunto 3/2022 del CEPD y el SEPD sobre la propuesta de Reglamento del Espacio Europeo de Datos Sanitarios (EEDS) [9].

En tercer lugar, y lo más importante a tener en cuenta en un futuro próximo, está el papel de los *intermediarios de datos*. Estos actores **median de algún modo entre los proveedores de datos, los interesados, los proveedores de almacenamiento de datos y los usuarios de datos**. Diferentes leyes europeas nuevas y futuras definen este tipo de entidades, por ejemplo, como intermediarios de datos en el Reglamento de Gobernanza de Datos [6] o como partes interesadas en la propuesta de Espacio Europeo de Datos Sanitarios [7].

Su función consiste normalmente en no utilizar ellos mismos los datos que comparten o, si lo hacen, solo para fines primarios muy limitados (como los hospitales que usan datos personales de los pacientes para prestarles servicios médicos esenciales). En su papel de intermediarios de datos, estos actores interactúan con los usuarios de datos, como las instituciones de investigación farmacéutica o las agencias de estadística, tratando de compartir datos con ellos teniendo en cuenta las fuentes de datos y los interesados. En términos del RGPD, pueden considerarse encargados del tratamiento de datos, pero su similitud con los usuarios de datos está aún por aclarar.

Figura 14: Escenario de compartición de datos con intermediarios



Como se indicó en un informe anterior de ENISA [10], la aplicación de los derechos de los interesados puede resultar difícil cuando se trata de un entorno distribuido de compartición de datos con múltiples actores, proveedores, subencargados del tratamiento, proveedores de servicios de TI, etc. Con los nuevos instrumentos jurídicos para los espacios de datos, este conjunto de usuarios de datos "directamente implicados" se amplía con nuevos actores, como las plataformas del sector privado para compartir datos, los mercados de datos, los depósitos

[12] Si el consentimiento (Art. 6(1)(a) GDPR) es la base legal para el tratamiento.

de datos alojados por el gobierno y otros tipos de intermediarios, tal como se indica en el Reglamento de Gobernanza de Datos.

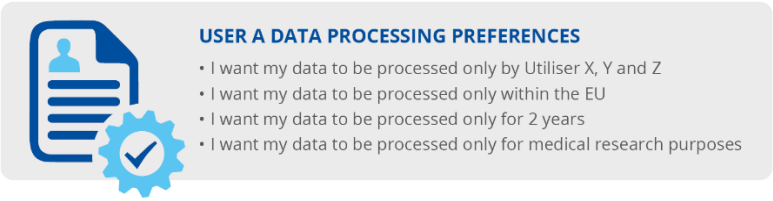
Estos actores no pretenden, en primer lugar, procesar ellos mismos esos datos, sino simplemente almacenarlos, alojarlos y proporcionarlos a los repositorios de datos bajo demanda. Según el Reglamento de Gobernanza de Datos, es deber explícito de estos actores atender y hacer cumplir los derechos de los interesados sobre los datos que están bajo su control. Por lo tanto, **requiere una definición clara de los permisos necesarios para acceder a dichos datos, que deben negociarse entre el interesado y el intermediario de datos, antes de cualquier actividad de intercambio de datos, y junto con ellas**.

4.1 INTERACCIÓN ENTRE EL INTERESADO Y EL INTERMEDIARIO DE DATOS

Un componente clave de todo tipo de tratamiento de datos personales es una base jurídica válida.[13] En la mayoría de los casos, suele ser el consentimiento explícito del interesado. A este respecto, el intermediario de datos tiene que encargarse de gestionar dicho consentimiento para el tratamiento de datos para cada uno de los usuarios de datos a los que sirve. Si un interesado declara su consentimiento para el tratamiento de sus datos personales en una organización, por ejemplo, esto no incluye automáticamente la transferencia a cualquier otra organización. Los interesados pueden optar por limitar su consentimiento a determinadas condiciones o abstenerse de darlo. Aunque el RGPD prescribe restricciones, p.ej. derivadas del principio de limitación de la finalidad, Art. 5(1)(b) del RGPD, las condiciones en las que un interesado puede facilitar voluntariamente información personal para determinados tipos de operaciones de tratamiento por parte de una o varias organizaciones pueden ser múltiples e incluso ir más allá de los criterios de protección de datos. La Figura 15 presenta algunos ejemplos que un interesado podría considerar.

Los interesados pueden optar por restringir su consentimiento solo a determinadas condiciones o, de lo contrario, pueden decidir abstenerse de darlo.

Figura 15: Ejemplo de preferencias de tratamiento de datos



Es evidente que la tarea de declarar y hacer cumplir tales políticas de tratamiento de datos en el intermediario de datos puede ser difícil. Requiere tanto una amplia interacción con el interesado, a fin de recabar y negociar todos los permisos de tratamiento necesarios, como una interacción con los repositorios de datos, a fin de validar la compatibilidad de las exigencias del interesado con las condiciones del usuario de datos. Por lo tanto, sería beneficioso disponer de un políticas y un modelo de datos explícitos, similares a los descritos en [33], [34] y [35] para definir dichas políticas de acceso.

Lo que hace que este reto sea aún más complejo son los posibles cambios a lo largo del tiempo; un interesado puede decidir, en cualquier momento, modificar arbitrariamente sus demandas de tratamiento de datos, o revocar el consentimiento para el tratamiento en determinados usuarios de datos. Por lo tanto, un intermediario de datos también tiene que hacer un seguimiento permanente de las solicitudes de cada interesado sobre el tratamiento en curso de los datos, con el fin de responder a un cambio de opinión de un interesado en un plazo razonable.

[13] Véase el art. 6(1)(a)-(f) RGPD, que enumera seis posibles motivos jurídicos.

4.1.1 Limitaciones de la finalidad

Un reto clave en este panorama es el aspecto de la limitación de la finalidad. Dado que un interesado puede elegir arbitrariamente restringir el tratamiento de sus propios datos para determinados fines, se hace necesario examinar más de cerca el ámbito de la compatibilidad de los fines. ¿Cómo puede un sistema de información ayudar a determinar si la autorización para el tratamiento de datos personales dada para un fin es compatible con el fin exacto del tratamiento por parte del usuario de los datos? ¿Qué puede hacerse para proporcionar a los intermediarios de datos la certidumbre necesaria y las garantías potenciales para que una compartición de datos que sea conforme con la protección de datos?

En el entorno actual de producción y usos de datos, existe una plétora de finalidades diferentes, que pueden ser o no compatibles, solaparse o incluirse entre sí. Además, existe un gran potencial de conflicto en caso de que la interpretación de los fines de estos permisos difiera entre los distintos agentes. Hay que prever que se necesitará algún tiempo y espacio para llegar a un enfoque algo consolidado y generalmente aceptado para tratar estas cuestiones del consentimiento y la finalidad vinculante en escenarios de intermediarios de datos.

4.1.2 Aspectos de la implementación

En el aspecto técnico de la ingeniería **la interacción entre los interesados y los intermediarios de datos puede realizarse de múltiples maneras**. Cuando los banners de política de cookies y sistemas similares de gestión de consentimiento son habituales, es posible dar y retirar el consentimiento, con interfaces técnicas más o menos funcionales que utilizar, por ejemplo, en [36] y [37]. Sin embargo, estos sistemas suelen formar parte de un sitio web con el que interactúa el interesado, y solo cubren los servicios que se ofrecen a través de este sitio web o de su proveedor de servicios. Por lo tanto, esto no resuelve los problemas que plantea la recogida del consentimiento en diferentes modos de interacción, p.ej. en coches inteligentes, para dispositivos portátiles o implantes médicos, o para otros sistemas de IoT que no ofrecen una interfaz de usuario razonable para el interesado [38] y [39].

Además, la mayoría de sistemas de gestión del consentimiento solo cubren un único sitio web o servicio de ámbito específico. No funcionan, o no lo hacen explícitamente, para los casos en los que la interacción inicial no la desencadena el interesado, sino simplemente un usuario de datos. Evidentemente, no es posible mostrar activamente un banner de consentimiento basado en un sitio web a un usuario que no esté interactuando en ese momento con el sitio web de un usuario de datos. Por lo tanto, si el inicio de una nueva actividad de tratamiento de datos no lo lleva a cabo el interesado sino el intermediario de datos, es necesario que exista un modo diferente de interacción entre el interesado y el intermediario de datos, en el que el intermediario de datos pueda ponerse en contacto proactivamente con el interesado para recabar un nuevo consentimiento para un nuevo caso de tratamiento de datos, p.ej. en un nuevo usuario de datos, o para una nueva finalidad del tratamiento de datos.

Retirar el consentimiento y comunicar las restricciones al tratamiento de datos son otros dos retos de esta interacción. Cada una de estas operaciones de tratamiento la desencadena inicialmente el interesado. **El enfoque común en este caso es que los datos sean suprimidos por el intermediario o el usuario, junto con una notificación activa dirigida al interesado.** Por lo tanto, en términos de ingeniería, la retirada del consentimiento o los derechos de rectificación, supresión o expresión de restricciones al tratamiento pueden gestionarse de forma similar proporcionando una interfaz de comunicación (como un sitio web), dirigida al interesado, que ofrezca estas interacciones como servicios.

Sin embargo, un reto para un intermediario de datos en estos casos es el de transmitir tales solicitudes a todos los usuarios de datos afectados. Esto requiere cierta gestión dentro del intermediario de datos y algunas interacciones con el usuario de datos. Empecemos por esto último.

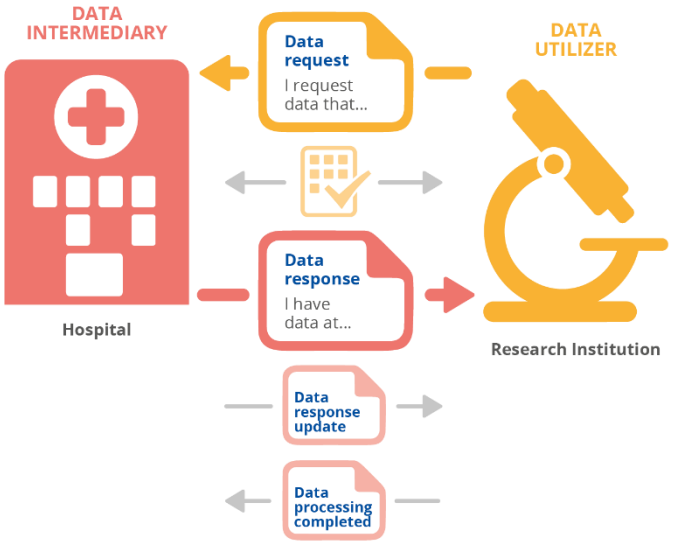
4.2
INTERACCIÓN ENTRE INTERMEDIARIOS Y USUARIOS DE DATOS

Una vez que los datos están disponibles en los repositorios del intermediario de datos, hay que considerar los detalles de los distintos modos de obtención de datos. Cuando un posible usuario de datos muestra interés por un subconjunto específico de los datos disponibles (o por el conjunto de datos en su totalidad), el intermediario de datos debe realizar varias tareas.

4.2.1 Solicitud y respuesta de datos

Inicialmente, un usuario de datos necesita poder dirigirse a un intermediario de datos, solicitando datos que pueden ser de naturaleza personal o no personal. En este último caso, pueden obviarse muchos de los pasos posteriores. En esa solicitud de datos, el usuario debe expresar los criterios específicos relativos a los datos que le interesan. Esto abarca, por ejemplo, atributos de los interesados cuyos datos se buscan, aspectos de tipos de datos, dominios, cantidades, calidades u orígenes, con una enorme plétora de diferentes tipos de filtros y restricciones a tener en cuenta. **El reto consiste en definir el formato y la sintaxis de una interacción con un grado suficiente de expresividad, para que el usuario de los datos pueda definir su demanda con la máxima precisión.**

Figura 16: Interacción entre el intermediario y el usuario de datos



Además de expresar los criterios de búsqueda de los datos que le interesan, **el usuario de los datos también tiene que definir con precisión la finalidad y el alcance del tratamiento de datos previsto**. El intermediario de datos necesita esta información para filtrar los conjuntos de datos en los que el interesado se haya opuesto de algún modo a tales tipos o ámbitos de tratamiento, o a tales tipos de destinatarios de datos. Por lo tanto, la información sobre, por ejemplo, los países en los que está previsto realizar el tratamiento de datos o los posteriores usuarios de datos por parte del usuario de datos debe comunicarse con un conjunto de atributos al intermediario de datos, a fin de que este pueda hacer cumplir la voluntad del interesado de manera fiable.

Sobre la base de esta solicitud inicial de datos, el intermediario de datos debe llevar a cabo un análisis interno para determinar los conjuntos de datos disponibles que se ajustan a los requisitos expresados por el usuario de datos. Como resultado, se identifica un conjunto de fuentes de datos, que podría servirse al usuario de datos como respuesta. Este conjunto de datos enviados como respuesta puede ser de tipo y cantidad bastante variados. A veces solo un subconjunto de datos de una tabla de base de datos podría cumplir todas las restricciones aplicables. A veces puede tratarse de una ubicación de almacenamiento de archivos, en la que

algunos archivos coinciden con los archivos de búsqueda y las políticas relativas a la finalidad. De nuevo, la respuesta debe ser capaz de hacer frente a una plétora de tipos de datos, formatos, sintaxis y tecnologías de acceso diferentes.

4.3 GESTIÓN DE DATOS EN EL INTERMEDIARIO DE DATOS

Para cumplir las necesidades y los derechos del interesado y del usuario de los datos, el intermediario de datos necesita hacer un seguimiento de todas las fuentes de datos y tareas de tratamiento de datos a la vez. Tiene que conocer e interactuar tanto con los interesados como con los usuarios de datos, según sea necesario, y tiene que evaluar y actualizar las políticas de uso de datos en múltiples etapas a lo largo del ciclo de vida del tratamiento de datos.

Como ya se ha dicho, el intermediario de datos debe almacenar los medios de comunicación de cada uno de los usuarios de datos con los que actúa, así como de la mayoría de los interesados. Cada nueva solicitud de tratamiento de datos debe ser registrada, rastreada y tratada razonablemente. Más allá de los tipos de acción necesarios con los interesados y los usuarios de datos, tal como se ha expuesto anteriormente, el intermediario de datos tiene que resolver algunos retos específicos, que se expondrán a continuación.

4.3.1 Cobertura del consentimiento y limitación de su finalidad

Una cuestión clave en el proceso de selección de los datos de un interesado que pueden cumplir o no los criterios establecidos por el usuario de datos es la del cumplimiento de los fines del tratamiento de datos. Si la base jurídica para el tratamiento de datos es el consentimiento, ¿cubre este consentimiento el ámbito del tratamiento previsto por el usuario de datos? Evidentemente, si el interesado ha incluido explícitamente al usuario de datos en una lista negra, la prueba de viabilidad es fácil: los datos de ese interesado no pueden formar parte de la respuesta al usuario de datos. Sin embargo, puede haber casos en que el intermediario de datos tenga que determinar —y decidir— si incluye o no estos datos en la respuesta; p.ej., para determinar si esa transferencia es compatible con la finalidad inicial del tratamiento de datos.

A veces, puede tratarse de una comparación de atributos en una lista explícita restricciones, como las identidades de los usuarios de los datos o los países de tratamiento, pero a veces, especialmente para los distintos fines del tratamiento, tal decisión no es tan trivial. **¿Cuándo está la finalidad definida por un usuario de datos para un caso concreto de tratamiento de datos suficientemente cubierta por las finalidades otorgadas por un interesado en su consentimiento?** Dependiendo de las condiciones exactas, el intermediario de datos tiene que decidir una de varias opciones diferentes sobre cómo proceder:

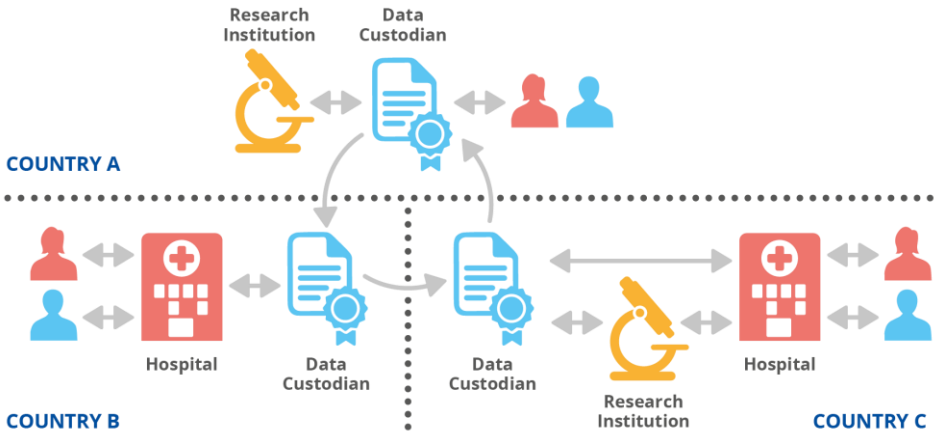
- incluir los datos, suponiendo que los fines sean claramente compatibles,
- excluir los datos, suponiendo que los fines sean claramente incompatibles,
- ponerse en contacto con el interesado para aclarar si los fines son compatibles o no, o para determinar si el interesado daría su consentimiento a la finalidad concreta del tratamiento en cuestión,
- consultar a terceros pertinentes, como las autoridades de protección de datos, para que le orienten sobre si los fines son compatibles o no.

4.3.2 Interacción entre intermediarios

A veces habrá más de un intermediario de datos implicado en la gestión de una solicitud de datos específica de un usuario de datos. En ese caso, o bien el usuario de datos pregunta a cada intermediario de datos por separado, dando lugar a situaciones como las comentadas anteriormente, o bien puede ser necesaria la interacción entre varios intermediarios de datos diferentes. Por ejemplo, **la decisión de incluir un determinado conjunto de datos en una respuesta puede ser tomada por un intermediario de datos, pero los datos en sí pueden estar controlados por otro intermediario de datos** (p.ej. un proveedor de almacenamiento

de datos). En tales casos, los intermediarios de datos tienen que interactuar en consecuencia para gestionar esa responsabilidad mixta – o conjunta–[14] de gestionar la solicitud de datos en consecuencia.

Figura 17: Intercambio transfronterizo de datos con custodios de datos



Un escenario específico para este tipo de interacción entre intermediarios de datos es el del intercambio transfronterizo de datos entre (y más allá de) los Estados miembros de la Unión Europea. En tales casos, la decisión sobre si los datos pueden salir de un país para ir a otro puede ser tomada, por ejemplo, por organizaciones nacionales especializadas en la custodia de datos o por tipos similares de intermediarios de datos. En tales casos, el protocolo de comunicación entre los intermediarios de datos tiene que atender también a esa demanda específica y a sus aspectos de comunicación, como se muestra en la Figura 17.

4.3.3 Registros e informes

Sea cual sea la solicitud de datos que se haga, sean cuales sean los datos que entren en el dominio de control de un intermediario de datos, el intermediario de datos tiene que hacer un seguimiento de ellos y rendir cuentas. Cuando se envía una respuesta a un usuario de datos, los detalles exactos del proceso de decisión sobre qué datos se han incluido deben almacenarse indefinidamente en el intermediario de datos, para poder informar más tarde al interesado, a los usuarios de datos, a los cuerpos y fuerzas de seguridad o a otras partes interesadas externas. Esto puede implicar requisitos legales para los intermediarios de datos con el fin de permitirles justificar cualquier actividad de compartición de datos en caso de que se presente una demanda.

4.3.4 Selección de datos para preservar la privacidad

Para cumplir su función de dar respuesta a las solicitudes de datos formuladas por los usuarios, el intermediario de datos debe conocer en profundidad todos los conjuntos de datos que controla. Esto puede incluso llegar a detalles como la revelación de datos individuales al intermediario de datos, por ejemplo, para determinar si atributos específicos del interesado en cuestión coinciden con las exigencias de filtrado de la solicitud de un usuario de datos. En ese caso, el problema de la privacidad y la confidencialidad de los datos frente al intermediario de datos se hace evidente. En su respuesta, ¿cómo puede el intermediario de datos decidir si incluir o no registros de datos individuales en un conjunto de datos sin tener acceso a los valores de filtrado de atributos dentro de los propios datos? **Una posible solución podría ser el cifrado basado en atributos (analizado en la Sección 2.1.1) o enfoques de seudonimización, como los analizados en** [16] **o incluso la anonimización**, que pueden

[14] Dependiendo de la aplicación real, puede constituir una situación de corresponsabilidad de acuerdo con el Art. 26 del RGPD.

ayudar a ocultar la identidad de los interesados tanto al intermediario como al usuario de los datos, siempre que no interfieran con la viabilidad de la propia actividad de tratamiento.

4.4 ALTRUISMO DE LOS DATOS

El concepto de cesión altruista de datos, también introducido en Reglamento de Gobernanza de Datos, se refiere a los interesados que aceptan el uso de sus datos para fines de interés general, como la investigación científica o la mejora de los servicios públicos. Por ejemplo, el altruismo de datos puede darse cuando un paciente decide permitir el tratamiento de los datos médicos recogidos sobre él no solo en el hospital, sino también por instituciones de investigación que desarrollan tratamientos. Lo interesante del altruismo es que normalmente no se da ninguna compensación al interesado. Sin embargo, esto no implica una renuncia de por vida a los derechos fundamentales a la intimidad y la protección de datos, tanto para el interesado como para la organización que procesa los datos.

El altruismo de datos, introducido en el Reglamento de Gobernanza de Datos, se refiere a los interesados que aceptan el uso sus datos para fines de interés general.

Por lo que respecta a la gestión de estos datos en un intermediario de datos, podría considerarse la posibilidad de marcar los datos como divulgados en virtud de una “licencia” de gestión de datos cedidos altruistamente, con el fin de abordar correctamente las demandas posteriores de los usuarios de datos con respecto a estos datos. Normalmente, siempre se conceden permisos de tratamiento de estos datos, pero la compartición de datos debe documentarse para poder demostrar la razón de la divulgación de los datos en caso de que el interesado presente una reclamación, por ejemplo, ante una autoridad de protección de datos en relación con los derechos de los interesados. En ese caso, el intermediario de datos debe poder demostrar el origen de los datos y los permisos iniciales dados por el interesado en ese momento.

5. CONCLUSIONES

Cuando dos o más partes deciden compartir sus datos, pasan a formar parte de un ecosistema de datos más amplio en el que pueden aprovechar el conjunto de datos combinados que permite descubrir, mediante el cálculo, nueva información o tendencias relativas a individuos, grupos de individuos, o a la sociedad en su conjunto. La forma más fácil y directa de alcanzar este objetivo sería compartir los datos brutos que posee cada actor a través de interfaces técnicas, poniéndolos en una tabla común (es decir, una única base de datos), pero esta hipotética opción no es realmente factible. En realidad, lo que buscamos son entornos compartidos de confianza que aprovechen al máximo el potencial que ofrece una compartición y un uso seguros de los datos personales, respetando al mismo tiempo los principios de protección de datos.

Este informe pretendía analizar casos concretos de uso compartido de datos personales, principalmente en el sector sanitario, y debatir cómo las tecnologías específicas y las consideraciones de aplicación pueden apoyar la ingeniería del uso compartido de datos personales en la práctica. El análisis abarcó desde la compartición de datos controlada por el usuario hasta la recopilación de datos personales a gran escala y la compartición de datos mediante servicios de terceros.

A pesar del potencial del concepto de compartición de datos y de la política y la legislación de la Unión en la materia, sigue habiendo consideraciones sobre cuáles son las medidas técnicas y organizativas adecuadas y cómo llevarlas a la práctica. Las iniciativas legislativas europeas en materia de compartición de datos descritas en la Sección 1.1 implican el tratamiento de grandes cantidades de datos que también incluirán datos personales. Por lo tanto, además de la coherencia de sus disposiciones con el RGPD, es importante eliminar cualquier inseguridad jurídica sobre las funciones y obligaciones, no solo para las personas físicas, como destacan el CEPD y la SEPD en [9], sino también para las entidades que participan en la compartición de datos. Para aprovechar el potencial de la compartición de datos en toda la UE, los profesionales podrían recibir orientaciones sobre qué tecnologías y técnicas pueden considerarse, en qué circunstancias y qué principios de protección de datos pueden cumplirse.

Existen varias técnicas (criptográficas) de uso común (a saber, cifrado asimétrico, seudónimos, control de acceso, etc.) que ya se reconoce que pueden paliar los riesgos de la protección de datos. Algunas de ellas se han analizado en la Sección 2, la Sección 3 y la Sección **¡Error! No se encuentra el origen de la referencia.**. Sin embargo, en conceptos emergentes como los espacios de datos y los intermediarios de datos, los riesgos planteados no siempre pueden abordarse adecuadamente solo con dichas técnicas. Esto se debe al hecho de que los interesados desean preservar la confidencialidad de los datos que comparten, pueden no saber de antemano con quién van a compartir datos o pueden querer compartir conjuntos de datos acumulados. Aunque existen técnicas avanzadas que aún están evolucionando, no deben considerarse de interés puramente académico, ya que existen implementaciones prácticas en escenarios de casos de uso reales.

Por último, dado que la mayoría de las tecnologías descritas anteriormente y en informes anteriores de ENISA [10] y [40] se basan en la criptografía asimétrica, debe preverse la llegada de la computación cuántica y su impacto en la seguridad de los cifrados asimétricos utilizados actualmente. Tras el despliegue de infraestructuras y servicios de intercambio de datos, no podemos esperar que dejen de funcionar debido a la posible inadecuación de los cifrados asimétricos. Aquí es donde la cripto-agilidad adquiere relevancia, ya que permite cambiar entre

algoritmos, primitivas criptográficas y otros mecanismos de cifrado sin cambios significativos en el sistema o proceso informático general.

REFERENCIAS

1. Xenos, H.: Latest trends in optical networks- straight from NGON & DCI World. (2019)

2. Data Protection Commission (DPC): Data Sharing in the Public Sector. (2019)

3. ICO: Data sharing: a code of practice. (2020)

4. Gartner: Data Sharing Is a Business Necessity to Accelerate Digital Business. (2021)

5. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "Una Estrategia Europea de Datos", COM/2020/66 final., Bruselas (2022)

6. Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) (2022)

7. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios (EEDS). (2022)

8. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas armonizadas para un acceso justo a los datos y su utilización (Ley de Datos). (2022)

9. CEPD-SEPD: Dictamen conjunto 3/2022 del CEPD y el SEPD sobre la propuesta de Reglamento del Espacio Europeo de Datos Sanitarios (EEDS). (2022)

10. ENISA: Ingeniería de la protección de datos. De la teoría a la práctica. (2022)

11. CEPD: Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto. (2019)

12. ENISA: Deploying Pseudonymisation Techniques: The case of the Health Sector. (2022)

13. Directiva 2011/24/UE del Parlamento Europeo y del Consejo de 9 de marzo de 2011 relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza. (2011)

14. Schwalbe, N., Wahl, B., Song, J., Lehtimaki, S.: Data Sharing and Global Public Health: Defining What We Mean by Data. Frontiers in Digital Health 2 (2020)

15. Hildebrandt, M., Verheul, E., Jacobs, B., Meijer, C., de Ruiter, J.: Polymorphic Encryption and Pseudonymisation for Personalised Healthcare: A Whitepaper., Cryptology ePrint Archive (2016)

16. ENISA: Pseudonymisation techniques and best practices. (2019)

17. Sahai, A., Waters, P.: Fuzzy Identity-Based Encryption. In : Advances in Cryptology – EUROCRYPT 2005, vol. 3494, pp.457-473 (2005)

18. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In : 13th ACM Conference on Computer and Communications Security, pp.89-98

19. Wang, F., Mickens, J., Zeldovich, N., Vaikuntanathan, V.: Sieve: Cryptographically Enforced Access Control for User Data in Untrusted Cloud. In : 13th

20. Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy cryptography. In : International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT 1998, pp.127-144 (1998)

21. Nuñez, D., Agudo, I., Lopez, J.: Proxy Re-Encryption: Analysis of constructions and its application to secure access delegation. Journal of Network and Computer Applications 87(1), 193-209 (2017)

22. Liang, X., Cao, Z., Lin, H., Shao, J.: Attribute based proxy re-encryption with delegating capabilities. In : 4th International Symposium on Information, Computer, and Communications Security, pp.276-286 (2009)

23. ENISA: Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation. (2019)

24. van Gastel, B., Jacobs, B., Popma, J.: Data Protection Using Polymorphic Pseudonymisation in a Large-Scale Parkinson's Disease Study., 19-25 (2021)

25. Verheul, E. .: The polymorphic eID scheme -combining federative authentication and privacy. (2019)

26. ENISA: Privacy and data protection in mobile applications. (2018)

27. Piotrowska, A., Hayes, J., Gelernter, N., Danezis, G.: AnNotify: A Private Notification Service., IACR eprint (2016)

28. Texto consolidado: Directiva 2010/13/UE del Parlamento Europeo y del Consejo de 10 de marzo de 2010 sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual) (2018)

29. ABC4Trust EU Project. Disponibl en: https://abc4trust.eu/

30. Piedra, A., Hoepman, J., Vullers, P.: Towards a Full-Featured Implementation of Attribute Based Credentials on Smart Cards. In : CANS 2014: Cryptology and Network Security, pp.270-289 (2014)

31. CNIL: Online age verification: balancing privacy and the protection of minors. (2022)

32. Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (2022)

33. McDonald, A., Reeder, R. W., Kelley, P. G., Cranor, L. F.: A Comparative Study of Online Privacy Policies and Formats. In : Privacy Enhancing Technologies Symposium, pp.37–55 (2009)

34. Drogkaris, P., Gritzalis, A., Lambrinoudakis, C.: Empowering Users to Specify and Manage Their Privacy Preferences in e-Government Environments. In : Electronic Government and the Information Systems Perspective, pp.237–245 (2014)

35. Hansen, M., Jensen, M.: A Generic Data Model for Implementing Right of Access Requests. In : APF 2022: Privacy Technologies and Policy, vol. 13279, pp.3-22 (3033)

36. Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., Holz, T.: We Value Your Privacy. Now Take Some Cookies. Informatik Spektrum, 345-346 (2019)

37. Karegar, F., Pettersson, J., Fischer-Hübner, S.: The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention. ACM Transactions on Privacy and Security 23(1), 1-38 (2020)

38. Castelluccia, C., Cunche, M., Le Metayer, D.: Enhancing Transparency and Consent in the IoT. In : 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp.116-119 (2018)

39. Murmann, P., Beckerle, M., Fischer-Hübner, S., Reinhardt, D.: Reconciling the what, when and how of privacy notifications in fitness tracking scenarios. Pervasive and Mobile Computing 77(C) (2021)

40. ENISA: Data Pseudonymisation: Advanced Techniques and Use Cases. (2021)

41. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (2016)

42. Alpár, G., Jacobs, B.: Credential Design in Attribute-Based Identity Management. (2013)

TP-03-22-200-EN-N

SOBRE ENISA

La Agencia de Ciberseguridad de la Unión Europea, ENISA, es la agencia de la Unión dedicada a lograr un alto nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada por el Reglamento sobre la Ciberseguridad de la UE, la Agencia de Ciberseguridad de la Unión Europea contribuye a la ciberpolítica de la UE, mejora la fiabilidad de los productos, servicios y procesos de las TIC con sistemas de certificación de la ciberseguridad, coopera con los Estados miembros y los organismos de la UE, y ayuda a Europa a prepararse para los retos cibernéticos del mañana. Mediante el intercambio de conocimientos, el desarrollo de capacidades y la sensibilización, la Agencia colabora con sus principales interesados para reforzar la confianza en la economía conectada, impulsar la resistencia de las infraestructuras de la Unión y, en última instancia, mantener la seguridad digital de la sociedad y los ciudadanos europeos. Puede encontrar más información sobre ENISA y su trabajo aquí: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-602-6
doi: 10.2824/36813