GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

0829/14/ES
WP216

Dictamen 05/2014 sobre técnicas de anonimización

Adoptado el 10 de abril de 2014

EL GRUPO DE TRABAJO SOBRE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

Vistos los artículos 29 y 30 de dicha Directiva,

Visto su reglamento interno,

HA ADOPTADO EL PRESENTE DICTAMEN:

RESUMEN

En este dictamen, el Grupo de Trabajo analiza la eficacia y las limitaciones de las técnicas de anonimización existentes, atendiendo al marco legal de la UE sobre protección de datos, y formula recomendaciones para la gestión de estas técnicas teniendo en cuenta el riesgo residual de identificación inherente a cada una de ellas.

El Grupo de Trabajo reconoce el valor potencial de la anonimización, en particular como estrategia para permitir a las personas y la sociedad en su conjunto beneficiarse de los «datos abiertos» al mismo tiempo que se mitigan los riesgos para los interesados. No obstante, los estudios de caso y las publicaciones científicas muestran la dificultad de crear un conjunto de datos verdaderamente anónimo conservando, sin embargo, toda la información subyacente requerida para la tarea.

A la luz de la Directiva 95/46/CE y de otros instrumentos jurídicos pertinentes de la UE, la anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación. En este proceso, los responsables del tratamiento deben considerar distintos aspectos y valorar todos los medios que puedan utilizarse «razonablemente» para la identificación de los datos (ya sea por el responsable del tratamiento o por terceros).

La anonimización implica un tratamiento posterior de los datos personales. Por tanto, debe satisfacer el requisito de compatibilidad teniendo en cuenta las circunstancias y los fundamentos jurídicos de dicho tratamiento. Por otra parte, aunque los datos anonimizados se encuentren fuera del alcance de la legislación sobre protección de datos, es posible que los interesados tengan derecho a protección en virtud de otras disposiciones legales (como las que protegen la confidencialidad de las comunicaciones).

En este documento se describen las principales técnicas de anonimización, a saber, la aleatorización y la generalización. En particular, se aborda el estudio de la adición de ruido, la permutación, la privacidad diferencial, la agregación, el anonimato k, la diversidad l y la proximidad t. Se exponen los principios en que se basan estos métodos, sus fortalezas y debilidades, y los errores más comunes al aplicar las distintas técnicas.

El dictamen expone la solidez de cada técnica aplicando tres criterios:

i) ¿Se puede singularizar a una persona?

ii) ¿Se pueden vincular registros relativos a una persona?

iii) ¿Se puede inferir información relativa a una persona?

Conocer las principales fortalezas y debilidades de cada técnica ayuda a comprender cómo diseñar un proceso de anonimización adecuado en un contexto dado.

En este documento se aborda también la seudonimización, para aclarar algunos errores e ideas falsas: la seudonimización no es un método de anonimización; simplemente, reduce la vinculabilidad de un conjunto de datos con la identidad original del interesado y es, en consecuencia, una medida de seguridad útil.

La conclusión del presente dictamen es que las técnicas de anonimización pueden aportar garantías de privacidad y usarse para generar procesos de anonimización eficientes, pero solo

si su aplicación se diseña adecuadamente, lo que significa que han de definirse con claridad los requisitos previos (el contexto) y los objetivos del proceso para obtener la anonimización deseada al mismo tiempo que se generan datos útiles. La solución óptima debe decidirse caso por caso y puede conllevar la combinación de diversas técnicas, aunque siempre respetando las recomendaciones prácticas que se formulan en este documento.

Por último, los responsables del tratamiento deben ser conscientes de que un conjunto de datos anonimizado puede entrañar todavía riesgos residuales para los interesados. Efectivamente, por una parte, la anonimización y la reidentificación son campos de investigación activos en los que se publican con regularidad nuevos descubrimientos y, por otra, incluso los datos anonimizados, como las estadísticas, pueden usarse para enriquecer los perfiles existentes de personas, con la consiguiente creación de nuevos problemas de protección de datos. En suma, la anonimización no debe contemplarse como un procedimiento esporádico, y los responsables del tratamiento de datos han de evaluar regularmente los riesgos existentes.

1 Introducción

Conforme aumentan los volúmenes de información y los tipos de datos que generan los dispositivos electrónicos, los sensores y las redes y se reduce el coste de almacenamiento hasta cantidades insignificantes, crecen el interés de los ciudadanos y la demanda de reutilización de estos datos. Unos «datos abiertos» pueden aportar beneficios visibles a la sociedad, a las personas y a las organizaciones, pero solo si se respetan los derechos de todos a la protección de los datos personales y a la vida privada.

La anonimización puede ser una buena estrategia para obtener estos beneficios al mismo tiempo que se mitigan los riesgos. Cuando un conjunto de datos se anonimiza realmente y no es posible ya identificar a las personas, no es aplicable la legislación europea de protección de datos. No obstante, los estudios de caso y las publicaciones científicas muestran claramente que la generación de un conjunto de datos verdaderamente anónimo a partir de un gran conjunto de datos personales, conservando al mismo tiempo la información subyacente que se requiere para llevar a cabo la tarea, no es un propósito sencillo. Por ejemplo, puede combinarse un conjunto de datos considerado anónimo con otro conjunto de datos de forma que sea posible identificar a una o más personas.

En este dictamen, el Grupo de Trabajo analiza la eficacia y las limitaciones de las técnicas de anonimización existentes, atendiendo al marco legal de la UE sobre protección de datos, y formula recomendaciones para el uso precavido y responsable de las mismas.

2 Definiciones y análisis jurídico

2.1. Definiciones en el contexto jurídico de la UE

En la Directiva 95/46/CE, el considerando 26 hace mención a la anonimización y excluye los datos anonimizados del alcance de la legislación sobre protección de datos:

> *«Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado;»*[1]

Una atenta lectura de este considerando permite obtener una definición conceptual de la anonimización. En virtud del mismo, para anonimizar cualesquiera datos es necesario eliminar de ellos los elementos suficientes para que no pueda identificarse al interesado. Con

[1] Asimismo, hay que señalar que este es el enfoque adoptado en el borrador del Reglamento europeo sobre la protección de datos, en cuyo considerando 23 se afirma que «para determinar si una persona es identificable deben tenerse en cuenta todos los medios que razonablemente pudiera utilizar el responsable del tratamiento o cualquier otra persona para identificar a dicha persona».

más precisión, hay que tratarlos de tal manera que no puedan usarse para identificar a una persona física mediante «el conjunto de los medios que puedan ser razonablemente utilizados» por el responsable del tratamiento o por terceros. Un factor importante al respecto es que el tratamiento debe ser irreversible. La Directiva no aclara cómo se debe o se puede llevar a cabo este proceso de desidentificación[2]. Se pone el acento en el resultado: los datos no deben permitir identificar al interesado mediante «el conjunto de los medios» que «puedan ser razonablemente» utilizados. Se hace referencia a los códigos de conducta como una herramienta para establecer posibles mecanismos de anonimización y de conservación de los datos de forma tal que «impida identificar al interesado». Por lo tanto, la Directiva establece claramente una norma muy rigurosa.

La Directiva sobre la protección de la intimidad en las comunicaciones electrónicas (Directiva 2002/58/CE) se refiere a la «anonimización» y los «datos anónimos» prácticamente en los mismos términos. El considerando 26 reza así:

> *Los datos sobre tráfico utilizados para la comercialización de los servicios de comunicaciones o para la prestación de servicios de valor añadido deben también eliminarse o hacerse anónimos tras la prestación del servicio.*

En el mismo sentido, el artículo 6, apartado 1, dispone lo siguiente:

> *Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.*

Y el artículo 9, apartado 1, señala lo siguiente:

> *En caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido.*

La idea subyacente es que el resultado de la anonimización, entendida esta como una técnica aplicada a los datos personales, debe ser, de acuerdo con el actual estado de la tecnología, tan permanente como el borrado. En otras palabras: debe garantizarse que es imposible tratar los datos personales[3].

---

[2] Esta idea se comentará con más detalle en la página 8 de este dictamen.

[3] Conviene recordar que el término «anonimización» también ha sido definido en normas internacionales, como ISO 29100, donde se afirma que es el proceso por el cual la información de identificación personal se modifica de forma irreversible de tal manera que el responsable del tratamiento no puede identificar, directa o indirectamente, ya sea por sus propios medios o en colaboración con algún tercero, a la persona asociada a dicha información de identificación personal (ISO 29100:2011). En las normas ISO, por tanto, lo esencial también es la irreversibilidad del proceso de modificación de los datos personales que permiten identificar directa o indirectamente al interesado. Desde este punto de vista, existe una importante convergencia entre esta postura y los principios y conceptos que forman la base de la Directiva 95/46/CE. Esto también es aplicable a las definiciones contenidas en las leyes de algunos países (por ejemplo, Italia, Alemania y Eslovenia), donde se pone el énfasis en la no identificabilidad y se hace referencia al «esfuerzo desproporcionado» para llevar a cabo la reidentificación (Alemania y Eslovenia). No obstante, la ley francesa de protección de datos dispone que los datos siguen siendo personales incluso en el caso de que la reidentificación del interesado sea extremadamente

2.2. Análisis jurídico

El análisis de las referencias a la anonimización en los principales instrumentos jurídicos de la UE sobre protección de datos permite poner de manifiesto cuatro características fundamentales:

- La anonimización puede ser el resultado de un tratamiento de datos personales realizado para impedir de forma irreversible la identificación del interesado.

- Pueden considerarse varias técnicas de anonimización, sin que la legislación europea contenga ninguna norma prescriptiva.

- Hay que dar importancia a los elementos contextuales: debe considerarse «el conjunto de los medios que puedan ser razonablemente utilizados» para la identificación por parte del responsable del tratamiento o de un tercero, prestando especial atención a lo que se entiende, en el estado actual de la técnica, como «medios que puedan ser razonablemente utilizados» (dado el incremento de la potencia de los ordenadores y de las herramientas disponibles).

- La anonimización lleva implícito un factor de riesgo que ha de tenerse en cuenta al evaluar la validez de las técnicas de anonimización, incluidos los posibles usos de los datos «anonimizados» mediante estas, además de considerarse asimismo la gravedad y probabilidad del riesgo.

En el presente dictamen, se usa el término «técnica de anonimización», en lugar de los términos «anonimato» o «datos anónimos», para subrayar el riesgo residual inherente de reidentificación vinculado a cualquier medida técnico-organizativa que tenga como objetivo la obtención de datos «anónimos».

2.2.1. Legitimación del proceso de anonimización

Ante todo, la anonimización es una técnica que se aplica a los datos personales para obtener una desidentificación irreversible. Por consiguiente, la premisa básica es que los datos personales deben haberse recogido y tratado de acuerdo con la legislación vigente sobre conservación de los mismos en un formato identificable.

En este contexto, el proceso de anonimización, entendido como el tratamiento de dichos datos personales para lograr su anonimización, es un caso particular de «tratamiento posterior». En consecuencia, este tipo de tratamiento debe cumplir la prueba de compatibilidad con arreglo a las directrices formuladas por el Grupo de Trabajo en su Dictamen 03/2013 sobre la limitación del fin[4].

Esto significa que, en principio, el fundamento jurídico de la anonimización puede encontrarse en cualquiera de los motivos mencionados en el artículo 7 (incluido el interés legítimo del responsable del tratamiento de datos), siempre que se cumplan además los requisitos de calidad relativos a los datos que se enumeran en el artículo 6 de la Directiva y

compleja e improbable. En otras palabras, no existe referencia alguna a la prueba de «razonabilidad» de los medios.

[4] Dictamen 03/2013 del Grupo de Trabajo del artículo 29, disponible en inglés en el siguiente vínculo: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

con la debida atención a las circunstancias específicas y la totalidad de los factores mencionados en el dictamen del Grupo de Trabajo sobre la limitación del fin[5].

Por otra parte, hay que destacar lo dispuesto en el artículo 6, apartado 1, letra e), de la Directiva 95/46/CE (así como en el artículo 6, apartado 1, y el artículo 9, apartado 1, de la Directiva sobre la protección de la intimidad en las comunicaciones electrónicas), ya que demuestra la necesidad de conservar los datos personales «en una forma que permita la identificación» durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

Esta disposición argumenta en favor de una anonimización de los datos personales por defecto (con sujeción a los diferentes requisitos legales aplicables, como los enunciados, en relación con los datos de tráfico, en la Directiva sobre la protección de la intimidad en las comunicaciones electrónicas). Si el responsable del tratamiento desea conservar estos datos personales una vez cumplidos los fines del tratamiento original o del tratamiento posterior, deberían usarse técnicas de anonimización para impedir de forma irreversible su identificación.

En consecuencia, el Grupo de Trabajo considera que la anonimización entendida como un caso particular de tratamiento posterior de datos personales puede considerarse compatible con el fin original del tratamiento, aunque solo con la condición de que el proceso de anonimización genere fiablemente información anonimizada en el sentido definido en este documento.

Debe subrayarse además que la anonimización ha de ajustarse a las restricciones legales que recuerda el Tribunal de Justicia de la Unión Europea en su sentencia sobre el asunto C-553/07 (*College van burgemeester en wethouders van Rotterdam contra M.E.E. Rijkeboer*) y que se refieren a la necesidad de conservar los datos en un formato identificable a fin de que puedan ejercerse, por ejemplo, los derechos de acceso por parte de los interesados. En concreto, el Tribunal señala que «*el artículo 12, letra a), de la Directiva [95/46/CE] obliga a los Estados miembros a garantizar un derecho de acceso a la información sobre los destinatarios o categorías de destinatarios a quienes se comunican los datos y al contenido de la información comunicada, no sólo para el presente, sino también para el pasado. Corresponde a los Estados miembros fijar un plazo de conservación de dicha información, así como el acceso correlativo a ésta, guardando un justo equilibrio entre, por un lado, el interés del afectado en proteger su intimidad, concretamente a través de las distintas vías de intervención y de recurso previstas por la Directiva y, por otro, la carga que la obligación de dicha información puede representar para el responsable del tratamiento*.»

Esto reviste una especial relevancia cuando, en lo que respecta a la anonimización, el responsable del tratamiento fundamente su actuación en el artículo 7, letra f), de la Directiva 95/46/CE: siempre debe guardarse un equilibrio entre el interés legítimo del responsable y los derechos y libertades fundamentales de los interesados.

[5] En particular, esto significa que es necesario llevar a cabo una evaluación sustantiva a la luz de las circunstancias relevantes, atendiendo especialmente a los siguientes factores clave:
a) la relación entre los fines para los que se recogieron los datos personales y los fines de su tratamiento posterior;
b) el contexto en el que se recogieron los datos personales y las expectativas razonables de los interesados en cuanto a su uso ulterior;
c) la naturaleza de los datos personales y el impacto del tratamiento ulterior en los interesados;
d) las salvaguardas adoptadas por el responsable del tratamiento para garantizar un tratamiento correcto e impedir cualquier tipo de efecto negativo indebido en los interesados.

Por ejemplo, una investigación llevada a cabo por las autoridades de protección de datos de los Países Bajos en 2012 y 2013 sobre el uso de tecnologías de inspección a fondo de paquetes (Deep Packet Inspection, DPI) por parte de cuatro operadores de telefonía móvil halló en el artículo 7, letra f), de la Directiva 95/46/CE el fundamento jurídico para la anonimización del contenido de los datos de tráfico a la mayor brevedad posible tras la recogida de estos. Efectivamente, el artículo 6 de la Directiva sobre la protección de la intimidad en las comunicaciones electrónicas establece que los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones públicas disponible al público deberán eliminarse o hacerse anónimos cuanto antes. En este caso, y dado que el artículo 6 de la Directiva sobre la protección de la intimidad en las comunicaciones electrónicas lo permite, el fundamento jurídico correspondiente se halla en el artículo 7 de la Directiva sobre protección de datos. La cuestión también podría plantearse a la inversa: si el artículo 6 de la Directiva sobre la protección de la intimidad en las comunicaciones electrónicas no permite un determinado tipo de tratamiento de datos, no puede encontrarse fundamento jurídico en el artículo 7 de la Directiva sobre protección de datos.

2.2.2. Identificabilidad potencial de los datos anonimizados

El Grupo de Trabajo examinó el concepto de «datos personales» en el Dictamen 4/2007 sobre datos personales, en el que se centra en los elementos componentes de la definición del artículo 2, letra a), de la Directiva 95/46/CE, entre ellos la referencia a una persona física «identificada o identificable». En este contexto, el Grupo de Trabajo llegó a la conclusión de que «los datos anonimizados serían, por tanto, datos anónimos que antes hacían referencia a una persona identificable, pero que ahora ya no admiten identificación».

Por consiguiente, el Grupo de Trabajo ya ha aclarado que la Directiva propone la razonabilidad de los medios usados («el conjunto de los medios que puedan ser razonablemente utilizados») como criterio para evaluar si el tratamiento de anonimización es suficientemente sólido, es decir, si la identificación es «razonablemente» imposible. Afectan directamente a la identificabilidad el contexto y las circunstancias particulares de cada caso. En el anexo técnico que acompaña a este dictamen, se analizan los efectos de la elección de la técnica más adecuada.

Como ya se ha señalado, hay una evolución continua de la investigación, las herramientas y la potencia de cálculo. Por ello, no es posible, ni tampoco útil, enumerar exhaustivamente las circunstancias en las que no se puede realizar la identificación. No obstante, merece la pena considerar e ilustrar algunos factores clave.

Primero, puede sostenerse que los responsables del tratamiento de los datos deben centrar su atención en los medios concretos que serían necesarios para revertir la técnica de anonimización, especialmente en lo que respecta al coste y a los conocimientos asociados al uso de dichos medios y a la evaluación de la probabilidad y gravedad de su uso. Por ejemplo, deberían comparar los esfuerzos y costes de la anonimización (en términos de tiempo y recursos requeridos) con la creciente disponibilidad de medios técnicos de bajo coste para identificar a las personas en conjuntos de datos, la cada vez mayor disponibilidad pública de otros conjuntos de datos (como los que se ofrecen en el marco de las políticas de «datos abiertos») y los numerosos casos de anonimización incompleta, que conllevan los consiguientes efectos adversos, a veces incluso irreparables, para los interesados[6]. Es

[6] Es interesante constatar que las enmiendas del Parlamento Europeo al proyecto de Reglamento general de protección de datos presentadas recientemente (21 de octubre de 2013), en el considerando 23, hacen mención

importante destacar que el riesgo de identificación puede aumentar con el tiempo y que también depende del desarrollo de las tecnologías de la información y la comunicación. Por lo tanto, las disposiciones legales correspondientes, de existir, deben formularse de manera tecnológicamente neutra y, idealmente, tener en cuenta los posibles cambios en la evolución de las tecnologías de la información[7].

Segundo, «el conjunto de los medios que puedan ser razonablemente utilizados para determinar si una persona es identificable o no» son los que serán utilizados «por el responsable del tratamiento o por cualquier otra persona». En consecuencia, es fundamental que comprendamos que, cuando el responsable del tratamiento no borra los datos originales (identificables) evento a evento y entrega parte de este conjunto de datos (por ejemplo, tras la eliminación o el enmascaramiento de los datos identificables), los datos resultantes siguen siendo datos personales. Tan solo si el responsable del tratamiento agrega los datos a un nivel en el que los eventos individuales dejan de ser identificables, el conjunto de datos resultantes puede calificarse de anónimo. Por ejemplo, si una organización recoge datos sobre los desplazamientos de personas, los patrones de viaje individuales a nivel de evento seguirían considerándose datos personales para cualquier parte mientras el responsable del tratamiento (o cualquier otra parte) siga teniendo acceso a los datos originales no tratados, aun en el caso de que se hayan eliminado los identificadores directos del conjunto entregado a terceros. Por el contrario, si el responsable del tratamiento borra los datos no tratados y entrega únicamente estadísticas agregadas a terceros a un nivel general (por ejemplo, «los lunes, en el trayecto X, hay un 160 % más de pasajeros que los martes»), entonces estaríamos hablando de datos anónimos.

Una solución de anonimización eficaz impide a todos singularizar a una persona en un conjunto de datos, vincular dos registros en un conjunto de datos (o dos registros pertenecientes a conjuntos diferentes) e inferir cualquier tipo de información a partir de dicho conjunto. En definitiva, como norma general, no basta con eliminar los elementos que pueden servir para identificar directamente a una persona para garantizar que ya no se puede identificar al interesado. Con frecuencia habrá que tomar medidas adicionales para evitar dicha identificación, las cuales dependerán una vez más del contexto y de los fines del tratamiento de que van a ser objeto los datos.

EJEMPLO:
Debido a su naturaleza única, los perfiles de datos genéticos constituyen un ejemplo de datos personales que están en riesgo de ser identificados si tan solo se utiliza la técnica de eliminación de la identidad del donante. Diversos estudios científicos ya han demostrado[8] que, al combinar los recursos genéticos disponibles para el público (p. ej., registros genealógicos, obituarios y resultados de consultas en motores de búsqueda) y los metadatos sobre donantes de ADN (fecha de donación, edad o lugar de residencia), se puede revelar la identidad de determinadas personas aunque el ADN se haya donado de forma «anónima».

Las dos familias de técnicas de anonimización (la aleatorización y la generalización)[9] tienen sus defectos. Aun así, en función de las circunstancias y el contexto, ambas pueden ser

expresa a que «para determinar si es razonablemente probable que unos medios se utilicen para identificar al individuo deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como el desarrollo tecnológico».

[7] Véase el Dictamen 4/2007 del Grupo de Trabajo del artículo 29, p. 15.

[8] Véase John Bohannon, Genealogy Databases Enable Naming of Anonymous DNA Donors, Science, Vol. 339, nº 6117 (18 de enero de 2013), p. 262.

[9] Las principales características de estas dos técnicas de anonimización y sus diferencias más destacadas se describen en la siguiente Sección 3 («Análisis técnico»).

adecuadas para alcanzar el fin deseado sin poner en riesgo la privacidad de los interesados. Es importante dejar claro que el concepto de «identificación» no conlleva únicamente la posibilidad de recuperar el nombre o la dirección de una persona, sino que incluye también la identificabilidad potencial por singularización, vinculabilidad o inferencia. Es más, a efectos legales es irrelevante la intención del responsable del tratamiento o del destinatario. Mientras los datos sean identificables, se aplica la legislación sobre protección de datos.

Un tercero puede tratar legítimamente un conjunto de datos sometido a una técnica de anonimización (es decir, un conjunto de datos anonimizados y entregados por el responsable del tratamiento original) sin obligación de sujetarse a los requisitos de protección de datos, siempre que no pueda identificar (directa o indirectamente) a los interesados en el conjunto de datos original. No obstante, el tercero está obligado a tener en cuenta los factores contextuales o circunstanciales mencionados anteriormente (entre los que se incluyen las características específicas de las técnicas de anonimización que el responsable del tratamiento original aplicara en su momento) al decidir cómo usar y, sobre todo, cómo combinar estos datos anonimizados para sus propios fines, dado que las consecuencias resultantes pueden acarrear algún tipo de responsabilidad por su parte. Cuando dichos factores y características entrañen un riesgo inaceptable de identificación de los interesados, el tratamiento entrará de nuevo en el ámbito de aplicación de la legislación sobre protección de datos.

La lista anterior no pretende ser exhaustiva, sino que aspira a servir de guía general para decidir cómo evaluar el potencial de identificabilidad de un conjunto de datos al que se le aplique la anonimización mediante cualquiera de las técnicas disponibles. Todos los factores citados anteriormente pueden considerarse como factores de riesgo que deben ser sopesados al anonimizar los conjuntos de datos (en el caso de los responsables del tratamiento) o cuando un tercero usa estos datos anonimizados para sus propios fines.

2.2.3. Riesgos del uso de datos anonimizados

Al considerar el uso de las técnicas de anonimización, los responsables del tratamiento de datos deben tener en cuenta los siguientes riesgos:

- Uno de los errores consiste en pensar que los datos seudonimizados son datos anonimizados. La sección «Análisis técnico» muestra que los datos seudonimizados no constituyen información anonimizada, ya que permiten singularizar a los interesados y vincularlos entre conjuntos de datos diferentes. La probabilidad de que el seudoanonimato admita la identificabilidad es muy alta; por ello, entra dentro del ámbito de aplicación del régimen jurídico de la protección de datos. Esto reviste una especial relevancia en el contexto de las investigaciones científicas, estadísticas e históricas[10].

EJEMPLO:
Un caso típico de las ideas erróneas sobre el concepto de seudonimización lo encontramos en el conocido «incidente AOL (America On Line)». En 2006 se publicó una base de datos con veinte millones de palabras clave de búsqueda y más de 650 000 usuarios correspondiente a un período de tres meses; la única medida que se tomó para preservar la intimidad fue reemplazar el identificador del usuario AOL por un atributo numérico. La consecuencia fue que se pudo identificar y localizar a algunos de los usuarios. Las cadenas de caracteres seudonimizadas de las consultas en los motores de búsqueda presentan una elevada capacidad de identificación, sobre todo si se asocian con otros atributos, como las direcciones IP u otros parámetros de configuración del cliente.

[10] Véase también el Dictamen 4/2007 del Grupo de Trabajo del artículo 29, pp. 18-20.

- Otro error consiste en pensar que los datos correctamente anonimizados, es decir, aquellos que satisfacen todas las condiciones y criterios mencionados anteriormente y que, por definición, quedan fuera del ámbito de aplicación de la Directiva sobre protección de datos, privan a las personas de cualquier tipo de protección, especialmente porque actos legislativos pueden ser aplicables al uso de estos datos. Por ejemplo, el artículo 5, apartado 3, de la Directiva sobre la protección de la intimidad en las comunicaciones electrónicas impide el almacenamiento de todo tipo de información (incluida la de carácter personal) y el acceso a la misma en los terminales sin el consentimiento del abonado o del usuario, ya que en este caso se aplica el principio general de la confidencialidad de las comunicaciones.

- Un tercer error sería olvidar los efectos en las personas que pueden tener, en determinadas circunstancias, los datos adecuadamente anonimizados, especialmente en el caso de la elaboración de perfiles de datos («profiling»). La esfera privada de la persona está protegida por el artículo 8 del Convenio Europeo de Derechos Humanos y el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea; en tal sentido, aunque no se aplique a este tipo de datos la legislación sobre protección de datos, el uso que se haga de los conjuntos de datos anonimizados que se entregan a terceros para que estos los usen para sus fines puede implicar una pérdida de privacidad. Hay que actuar con especial precaución al manejar información anonimizada, especialmente cuando esta se utiliza (con frecuencia en combinación con otros datos) para tomar decisiones que causan efectos (aunque sea indirectamente) en las personas. Tal y como se señala en este dictamen, y como ha puesto de manifiesto con toda claridad el Grupo de Trabajo, en particular, en el dictamen sobre el concepto de «limitación del fin» (Dictamen 03/2013)[11], las expectativas legítimas de los interesados en lo que respecta al tratamiento posterior de sus datos deben evaluarse a la luz de los factores contextuales relevantes, como la naturaleza de la relación entre ellos y los responsables del tratamiento, las obligaciones legales aplicables o la transparencia de las operaciones de tratamiento.

3 Análisis técnico, solidez de las tecnologías y errores típicos

Existen diversas prácticas y técnicas de anonimización con diferentes grados de solidez. Esta sección aborda los principales aspectos que los responsables del tratamiento deben considerar al aplicarlas. Hay que valorar, en particular, la garantía que se obtiene al aplicar una determinada técnica, teniendo en cuenta el estado actual de la técnica y los tres riesgos clave de la anonimización:

- *Singularización*: la posibilidad de extraer de un conjunto de datos algunos registros (o todos los registros) que identifican a una persona.
- *Vinculabilidad*: la capacidad de vincular como mínimo dos registros de un único interesado o de un grupo de interesados, ya sea en la misma base de datos o en dos bases de datos distintas. Si el atacante puede determinar (p. ej., mediante un análisis de correlación) que dos registros están asignados al mismo grupo de personas pero no puede singularizar a las personas en este grupo, entonces la técnica es resistente a la singularización, pero no a la vinculabilidad.
- *Inferencia*: la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos.

[11] Disponible en inglés en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Por consiguiente, una estrategia que prevenga estos tres riesgos tendrá la solidez necesaria para impedir la reidentificación de los datos mediante los medios más probables y razonables que puedan emplear el responsable del tratamiento y cualquier tercero. A este respecto, el Grupo de Trabajo quiere señalar que se realizan numerosos estudios científicos sobre las técnicas de desidentificación y anonimización. Estas investigaciones ponen claramente de manifiesto que no hay ninguna técnica infalible. En términos generales, existen dos enfoques diferentes de la anonimización: el primero se basa en la ***aleatorización***; el segundo, en la ***generalización***. Este dictamen también examina otros conceptos, como la *seudonimización, la privacidad diferencial, la diversidad l y la proximidad t.*

Indicamos a continuación los términos que se utilizarán en esta sección. Un conjunto de datos está formado por diferentes registros relativos a personas (los interesados). Cada registro hace referencia a un interesado y contiene una serie de valores (también llamados entradas, p. ej., «2013») para cada atributo (p. ej., «año»). Un conjunto de datos está formado por una serie de registros y puede adoptar forma de tabla (o de un conjunto de tablas) o de gráfico anotado o ponderado, que es la opción que se utiliza cada vez más. Los ejemplos incluidos en este documento se refieren a tablas, pero también son aplicables a otros tipos de representación gráfica de registros. En ocasiones se utilizará el término cuasi identificadores para referirse a las combinaciones de atributos que hacen referencia a un interesado o a un grupo de interesados. En algunos casos, un conjunto de datos puede contener varios registros relativos a la misma persona. Un atacante es un tercero (es decir, no es ni el responsable del tratamiento ni el encargado del tratamiento) que accede a los registros originales de manera accidental o intencionada.

3.1. Aleatorización

La aleatorización es una familia de técnicas que modifican la veracidad de los datos a fin de eliminar el estrecho vínculo existente entre los mismos y la persona. Si los datos se hacen lo suficientemente ambiguos, no podrán remitir a una persona concreta. La aleatorización por sí sola no reduce la singularidad de cada uno de los registros, ya que estos pueden obtenerse a partir de un único interesado, pero sí puede proteger contra ataques o riesgos de inferencia. Además, se puede combinar con técnicas de generalización para obtener mayores garantías de privacidad. Es posible que haya que aplicar otras técnicas para garantizar que un registro no sirve para identificar a una persona.

3.1.1. Adición de ruido

La técnica de adición de ruido es especialmente útil cuando los atributos pueden causar un importante efecto adverso en las personas. Consiste en modificar los atributos del conjunto de datos para que sean menos exactos, conservando no obstante su distribución general. Al tratar un conjunto de datos, cualquier observador supondrá que los valores son exactos, pero esto solo es cierto hasta cierto punto. Por ejemplo, aunque la altura de una persona se mida originalmente hasta el centímetro más próximo, el conjunto de datos anonimizado puede contener valores con una exactitud de ± 10 cm. Si se utiliza esta técnica de manera competente, un tercero no podrá identificar a una persona ni tampoco debería ser capaz de restaurar los datos o de averiguar cómo se han modificado.

Normalmente, la adición de ruido debe combinarse con otras técnicas de anonimización, como la eliminación de atributos obvios y de cuasi identificadores. El nivel de ruido depende de la cantidad y el tipo de información que se requiera, así como del impacto que tenga la revelación de los atributos protegidos en la privacidad de las personas.

3.1.1.1. Garantías

- *Singularización:* Se pueden singularizar los registros de una persona (quizá de manera no identificable), aunque sean menos fiables.
- *Vinculabilidad:* Se pueden vincular los registros de una misma persona, pero estos son menos fiables, por lo cual se puede vincular un registro real con uno añadido artificialmente (es decir, vincularlo con el ruido). En algunos casos, una atribución incorrecta puede exponer al interesado a un nivel de riesgo significativo, incluso mayor que en el caso de una atribución correcta.
- *Inferencia:* Se pueden llevar a cabo ataques por inferencia, pero la tasa de éxito será menor; además, no se descartan falsos positivos (o falsos negativos).

3.1.1.2. Errores frecuentes

- Añadir ruido inconsistente: Si el ruido no es semánticamente viable (es decir, está fuera de escala y no respeta la lógica entre los atributos de un conjunto de datos), un atacante que acceda a la base de datos podrá filtrar el ruido y, en algunos casos, recuperar la entradas que faltan. Es más, si existen pocos elementos en el conjunto de datos[12], persistirá la posibilidad de vincular las entradas de datos con ruido con una fuente externa.
- Pensar que la adición de ruido es una medida suficiente: La adición de ruido es una medida complementaria que hace más difícil que un atacante se haga con los datos personales. A no ser que el ruido sea mayor que la información contenida en el conjunto de datos, jamás debería pensarse que la adición de ruido es una solución completa para la anonimización.

3.1.1.3. Defectos de la adición de ruido

Un experimento de reidentificación muy famoso es el que se llevó a cabo con la base de datos de clientes del proveedor de contenidos de vídeo Netflix. Los investigadores analizaron las propiedades geométricas de esta base de datos, que está formada por más de 100 millones de valoraciones de unas 18 000 películas en una escala de 1 a 5 por parte de 500 000 usuarios. La empresa hizo pública esta base de datos tras anonimizarla con arreglo a sus directrices internas sobre privacidad. En concreto, eliminó todo tipo de información que pudiera identificar al cliente, excepto las valoraciones y las fechas. Se añadió ruido a las valoraciones mejorándolas o empeorándolas ligeramente.

A pesar de ello, se descubrió que se podía identificar de manera unívoca el 99 % de los registros de usuarios en el conjunto de datos usando 8 valoraciones y fechas con errores de 14 días a modo de criterio de selección. Aun rebajando los criterios de selección a 2 valoraciones y un error de 3 días, se podía identificar al 68 % de los usuarios[13].

3.1.2. Permutación

Esta técnica consiste en mezclar los valores de los atributos en una tabla para que algunos de ellos puedan vincularse artificialmente a distintos interesados. Se trata de una estrategia útil

[12] Esta idea se comenta con más detalle en la página 30 del anexo de este documento.
[13] Narayanan, A., y Shmatikov, V. (2008, Mayo). Robust de-anonymization of large sparse datasets. En *Security and Privacy, 2008. SP 2008. IEEE Symposium on* (pp. 111-125). IEEE.

en el caso de que sea importante conservar la distribución exacta de cada atributo en el conjunto de datos.

La permutación puede considerarse como una forma de adición de ruido. En la forma clásica de adición de ruido, los atributos se sustituyen por valores aleatorizados. Generar un ruido consistente puede ser una tarea difícil, aparte de que, si la modificación de los valores de los atributos es mínima, puede que no se obtenga el grado de privacidad deseado. Con las técnicas de permutación, se intercambian los valores contenidos en el conjunto de datos, trasladándolos de un registro a otro. Esta permuta de datos garantiza que el rango y la distribución de valores sean idénticos, no así las correlaciones entre los valores y las personas. Si dos o más atributos tienen una relación lógica o una correlación estadística y se permutan independientemente del resto, dicha relación quedará destruida. Por consiguiente, sería importante permutar un conjunto de atributos que estén relacionados entre sí a fin de no romper la relación lógica. En caso contrario, un atacante podría identificar los atributos permutados y revertir la permutación.

Por ejemplo, imaginemos el siguiente subconjunto de atributos en un conjunto de datos médicos: «razones para la hospitalización», «síntomas» y «servicio hospitalario responsable». En la mayoría de los casos, existirá una estrecha relación lógica entre los valores, de modo que si se llevara a cabo la permutación en uno solo de estos valores, esta técnica sería detectada e incluso podría revertirse.

Al igual que ocurre con la adición de ruido, la permutación por sí sola no permite obtener la anonimización, por lo que siempre debe combinarse con el procedimiento de eliminación de atributos obvios o cuasi identificadores.

3.1.2.1. Garantías

- *Singularización:* Igual que con la adición de ruido, aún se pueden identificar los registros de una persona, aunque los registros son menos fiables.
- *Vinculabilidad:* Si la permutación se aplica a atributos y cuasi identificadores, es posible que impida la vinculación «correcta» de atributos tanto dentro como fuera de un conjunto de datos, pero todavía podría darse una vinculación «incorrecta», ya que una entrada real puede asociarse a un interesado distinto.
- *Inferencia:* Es posible realizar inferencias a partir del conjunto de datos, especialmente si existe una correlación entre los atributos o tienen relaciones lógicas muy estrechas. No obstante, como el atacante desconoce qué atributos se han permutado, debe asumir que su inferencia se basa en una hipótesis equivocada y, por lo tanto, tan solo puede recurrir a una inferencia basada en probabilidades.

3.1.2.2. Errores frecuentes

- Seleccionar el atributo equivocado: Si se permutan atributos no sensibles o que no entrañan riesgo de identificación alguno, no se obtendrá un beneficio significativo en términos de protección de datos personales. Efectivamente, si los atributos sensibles o que entrañan riesgo de identificación siguen asociados al atributo original, el atacante podría extraer información sensible sobre las personas.
- Permutar los atributos de manera aleatoria: Si existe una fuerte correlación entre dos atributos, la permutación aleatoria de estos atributos no proporciona garantías suficientes. Este error tan frecuente se ilustra en la tabla 1.

- Pensar que la permutación es una medida más que suficiente: Igual que ocurre con la adición de ruido, la permutación por sí sola no permite alcanzar el anonimato, por lo que siempre debe combinarse con otras técnicas, como la eliminación de atributos obvios.

3.1.2.3. Insuficiencias de la permutación

El siguiente ejemplo muestra que, si se permutan los atributos aleatoriamente, no se puede garantizar la intimidad si existen vínculos lógicos entre atributos diferentes. Tras realizar el intento de anonimización, resulta sencillo deducir los ingresos de cada persona en función de su trabajo y año de nacimiento. Por ejemplo, tras examinar los datos, se puede afirmar que el Director Ejecutivo que aparece en la tabla muy probablemente nació en 1957 y disfruta del salario más alto, mientras que el desempleado nació en 1964 y tiene los menores ingresos.

Año	Sexo	Cargo	Ingresos (permutados)
1957	M	Ingeniero	70k
1957	M	Director Ejecutivo	5k
1957	M	Desempleado	43k
1964	M	Ingeniero	100k
1964	M	Gerente	45k

Tabla 1: Un ejemplo ineficaz de anonimización mediante permutación de atributos correlacionados.

3.1.3. Privacidad diferencial

La privacidad diferencial[14] pertenece a la familia de técnicas de aleatorización, aunque adopta un enfoque diferente. Mientras que, en la práctica, la inserción de ruido tiene lugar antes del momento en que se prevé difundir el conjunto de datos, la privacidad diferencial, por el contrario, puede usarse cuando el responsable del tratamiento de datos genera vistas anonimizadas de un conjunto de datos, al mismo tiempo que conserva una copia de los datos originales. Estas vistas anonimizadas normalmente se generan mediante un subconjunto de consultas de un determinado tercero. Este subconjunto contiene algo de ruido aleatorio que se añade de manera deliberada con posterioridad. La privacidad diferencial indica al responsable del tratamiento cuánto ruido debe añadir, y en qué forma, para obtener las garantías de privacidad necesarias[15]. En este contexto, es especialmente importante una supervisión continua (como mínimo de cada nueva consulta) para evaluar cualquier posibilidad de identificación de una persona en el conjunto de resultados de las consultas. Sin embargo, conviene aclarar que las técnicas de privacidad diferencial no modifican los datos originales. Por lo tanto, mientras se conserven los datos originales, el responsable del tratamiento es capaz de identificar a las personas a partir de los resultados de las consultas de privacidad diferencial mediante el conjunto de los medios que pueden ser razonablemente utilizados. Estos resultados también deben considerarse como datos personales.

[14] Dwork, C. (2006). Differential privacy. En *Automata, languages and programming* (pp. 1-12). Springer Berlin Heidelberg.

[15] Cf. Ed Felten (2012) Protecting privacy by adding noise. URL (en inglés): https://techatftc.wordpress.com/2012/06/21/protecting-privacy-by-adding-noise/.

Una de las ventajas del enfoque basado en la privacidad diferencial consiste en el hecho de que los conjuntos de datos se entregan a terceros autorizados como respuesta a una consulta concreta y no simplemente como consecuencia de la publicación de un único conjunto de datos. Para que el control sea más sencillo, el responsable del tratamiento puede conservar una lista de todas las consultas y solicitudes a fin de garantizar que los terceros no acceden a datos que no están autorizados a consultar. A una consulta también se le pueden aplicar técnicas de anonimización, incluidas la adición de ruido y la sustitución, al objeto de aumentar la protección de la privacidad. Encontrar un buen mecanismo interactivo de consulta-respuesta que sea capaz de contestar cualquier pregunta con cierta precisión (en la manera menos ruidosa posible) y que, al mismo tiempo, pueda preservar la privacidad, sigue siendo objeto de investigación.

Para reducir los ataques por inferencia y vinculabilidad, es necesario hacer un seguimiento de las consultas lanzadas por una entidad y examinar la información sobre los interesados que se obtiene. Por ello, las bases de datos con intimidad diferencial no deberían utilizarse con motores de búsqueda abiertos que no permitan la trazabilidad de las entidades que formulan las consultas.

3.1.3.1 Garantías

- *Singularización:* Si la salida está formada exclusivamente por datos estadísticos y las reglas que se aplican al conjunto se han escogido adecuadamente, no debería ser posible usar las respuestas para singularizar a una persona.
- *Vinculabilidad:* Si se lanzan varias consultas, es posible que se puedan vincular las entradas relativas a una persona determinada entre dos respuestas.
- *Inferencia:* Se puede inferir información sobre personas o grupos lanzando varias consultas.

3.1.3.2. Errores frecuentes

- No añadir ruido suficiente: Para evitar la vinculación con conocimientos previos que se posea sobre los interesados, el reto consiste en evitar que se pueda traslucir si un interesado o un grupo de interesados en particular ha aportado información o no al conjunto de datos. Desde el punto de vista de la protección de datos, la mayor dificultad estriba en ser capaces de generar la cantidad adecuada de ruido que se añade a las respuestas verdaderas a fin de proteger la privacidad de las personas y, al mismo tiempo, preservar la utilidad de las respuestas difundidas.

3.1.3.3 Insuficiencias de la privacidad diferencial

Tratar cada consulta de forma independiente: Si se combinan los resultados de varias consultas, se podría obtener información secreta. Si no se conserva un historial de las consultas, el atacante podría diseñar una batería de preguntas a una base de datos con privacidad diferencial que fuera reduciendo progresivamente la extensión de las respuestas obtenidas hasta que surgiera un carácter determinado de un interesado o de un grupo de interesados en particular, de forma determinista o con una alta probabilidad. Además, conviene tener la precaución de no caer en el error de pensar que los datos son anónimos para el tercero cuando el responsable del tratamiento todavía puede identificar al interesado en la base de datos original mediante el conjunto de medios que pueden ser razonablemente utilizados.

3.2. Generalización

La generalización es la segunda familia de técnicas de anonimización. Este enfoque generaliza o diluye los atributos de los interesados modificando las respectivas escalas u órdenes de magnitud (por ejemplo, sustituyendo una ciudad por una región, o una semana por un mes). Aunque la generalización pueda ser efectiva para descartar la singularización, no permite obtener una anonimización eficaz en todos los casos; en concreto, es necesario aplicar enfoques cuantitativos específicos y complejos para impedir la vinculabilidad y la inferencia.

3.2.1. Agregación y anonimato k

Las técnicas de agregación y anonimato k tienen el objetivo de impedir que un interesado sea singularizado cuando se le agrupa junto con, al menos, un número k de personas. Para lograrlo, los valores de los atributos se generalizan hasta el punto de que todas las personas acaban compartiendo el mismo valor. Por ejemplo, al reducir la granularidad de un lugar (de ciudad a región), muchos interesados compartirán esos valores. Las fechas de nacimiento pueden generalizarse en períodos de tiempo, o bien agruparse por mes o año. Otros atributos numéricos (p. ej., salario, peso, altura y dosis de medicina), pueden generalizarse por intervalos de valores (p. ej.: salario, entre 20 000 y 30 000 euros). Estos métodos son aplicables cuando la correlación de valores puntuales de atributos puede crear cuasi identificadores.

3.2.1.1. Garantías

- *Singularización:* Dado que ahora hay k usuarios que comparten los mismos atributos, ya no se puede singularizar a una persona entre un grupo de k usuarios.
- *Vinculabilidad:* Aunque la vinculabilidad es remota, aún se pueden vincular registros por grupos de k usuarios. Por tanto, dentro de ese grupo, la probabilidad de que dos registros se correspondan con los mismos seudoidentificadores es de 1/k. Puede que este valor sea considerablemente mayor que la probabilidad de que dichas entradas no sean vinculables.
- *Inferencia:* El defecto principal del modelo de anonimato k es que no impide los ataques por inferencia. Cuando las k personas pertenecen al mismo grupo, si se conoce a qué grupo pertenece una persona determinada, resulta sencillo recuperar el valor de esta propiedad.

3.2.1.2. Errores frecuentes

- Perder algunos cuasi identificadores: Al considerar el anonimato k, uno de los parámetros críticos es el umbral de k. Cuanto más alto sea este valor, más garantías de privacidad obtendremos. Un error frecuente consiste en aumentar el valor de k de manera artificial reduciendo el conjunto de los cuasi identificadores considerados. Cuando se reduce el número de cuasi identificadores, es más fácil construir clústeres de k usuarios debido al poder inherente de identificación asociado al resto de atributos, sobre todo si algunos de ellos son sensibles o poseen una entropía muy elevada, como en el caso de atributos muy raros. No considerar la totalidad de los identificadores cuando se escoge el atributo que se va a generalizar es un error crítico; si se pueden utilizar algunos atributos para singularizar a una persona en un clúster de k usuarios, algunas personas no estarán protegidas por la generalización (véase el ejemplo de la tabla 2).

- Valor pequeño de k: Intentar obtener un valor pequeño de k es igual de problemático. Si k es demasiado bajo, el peso de cualquier persona en un clúster es considerable, por lo que los ataques por inferencia obtienen mayores tasas de éxito. Por ejemplo: si k=2, la probabilidad de que las dos personas compartan la misma propiedad es mayor que para k > 10.
- No agrupar a las personas que tengan el mismo peso: Agrupar a un conjunto de personas mediante una distribución no uniforme de los atributos también puede causar problemas. Los efectos de un registro de una persona en el conjunto de datos pueden ser diversos. Algunos representarán una fracción importante de las entradas, mientras que la contribución de otros será prácticamente inapreciable. Por consiguiente, es importante asegurarse de que k es lo suficientemente alto como para que no haya ninguna persona que represente una fracción considerable de las entradas de un clúster.

3.1.3.3. Insuficiencias del anonimato k

La principal laguna del anonimato k es que no impide los ataques por inferencia. En el siguiente ejemplo, si el atacante sabe que una determinada persona está contenida en el conjunto de datos y que ha nacido en 1964, también sabrá que ha muerto por un infarto. Es más, si sabemos que este conjunto de datos pertenecía a una organización francesa, sabremos que cada una de estas personas reside en París, ya que el código postal de esta ciudad comienza por 750.

Año	Sexo	CP	Diagnóstico
1957	M	750*	Infarto
1957	M	750*	Colesterol
1957	M	750*	Colesterol
1964	M	750*	Infarto
1964	M	750*	Infarto

Tabla 2: Ejemplo de una anonimización k diseñada defectuosamente.

3.2.2. Diversidad l, proximidad t

La diversidad l extiende el anonimato k para garantizar que ya no se puedan realizar ataques por inferencia deterministas. Para ello, se asegura de que en cada clase de equivalencia, todos los atributos tienen al menos *l* valores diferentes.

Uno de los objetivos fundamentales consiste en limitar la ocurrencia de clases de equivalencia que tengan una variabilidad de atributos escasa. De esta forma, un atacante que posea conocimientos previos sobre un interesado en concreto siempre estará sometido a un grado significativo de incertidumbre.

La diversidad l es útil para proteger los datos ante ataques por inferencia, siempre que los valores de los atributos estén bien distribuidos. No obstante, conviene señalar que esta técnica no puede evitar la filtración de información si los atributos de una partición se distribuyen de manera no uniforme o pertenecen a un rango de valores o significados semánticos muy estrecho. En última instancia, la diversidad l está sujeta a ataques por inferencia probabilísticos.

La proximidad t es un perfeccionamiento de la diversidad l. Consiste en crear clases equivalentes que se parezcan a la distribución inicial de los atributos en la tabla. Esta técnica es útil cuando haya que conservar los datos lo más próximo posible a los originales. Para ello, se añade una nueva restricción a la clase de equivalencia: no basta con que existan al menos *l* valores diferentes en cada clase de equivalencia, sino que, además, cada valor debe representarse tantas veces como sea necesario a fin de reflejar la distribución inicial de cada atributo.

3.2.2.1. Garantías

- *Singularización:* Igual que ocurre con el anonimato k, la diversidad l y la proximidad t garantizan que los registros relativos a una persona no se puedan singularizar en la base de datos.
- *Vinculabilidad:* La diversidad l y la proximidad t no mejoran el anonimato k en lo que se refiere a la no vinculabilidad. Se da el mismo problema que con cualquier clúster: la probabilidad de que las mismas entradas pertenezcan al mismo interesado es mayor que 1/N (donde N es el número de interesados en la base de datos).
- *Inferencia:* La principal mejora que ofrecen la diversidad l y la proximidad t con respecto al anonimato k es que ya no se pueden llevar a cabo ataques por inferencia contra una base de datos con diversidad l o proximidad t con un cien por ciento de confianza.

3.2.2.2. Errores frecuentes

- Proteger valores de atributos sensibles mezclándolos con otros atributos sensibles: Para garantizar la privacidad, no basta con tener dos valores de un atributo en un clúster. De hecho, la distribución de valores sensibles en cada clúster debería ser similar a la distribución de dichos valores en la población total, o al menos debería ser uniforme en el clúster.

3.2.2.3. Insuficiencias de la diversidad l

En la tabla que se muestra a continuación, existe diversidad l para el atributo «Diagnóstico». No obstante, si se supiera que una persona nacida en 1964 aparece en esta tabla, se podría deducir que, muy probablemente, sufrió un infarto.

Año	Sexo	CP	Diagnóstico
1957	M	750*	**Infarto**
1957	M	750*	**Colesterol**
1957	M	750*	**Colesterol**
1957	M	750*	**Colesterol**
1964	M	750*	**Infarto**
1964	M	750*	**Infarto**
1964	M	750*	**Infarto**
1964	M	750*	**Colesterol**
1964	M	750*	**Infarto**
1964	M	750*	**Infarto**
1964	M	750*	**Infarto**
1964	M	750*	**Infarto**
1964	M	750*	**Infarto**
1964	M	750*	**Infarto**
1964	M	750*	**Infarto**

Tabla 3: Tabla con diversidad l cuyos valores para el atributo «Diagnóstico» no se han distribuido de manera uniforme.

Nombre	Fecha de nacimiento	Sexo
Smith	1964	M
Rossi	1964	M
Dupont	1964	M
Jansen	1964	M
García	1964	M

Tabla 4: Si un atacante supiera que estas personas están en la tabla 3, podría inferir que sufrieron un infarto.

4. Seudonimización

La seudonimización consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro. Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo. No obstante, el presente dictamen examina este método debido a las numerosas ideas falsas y errores existentes sobre él.

La seudonimización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado; se trata, por tanto, de una medida de seguridad útil, pero no es un método de anonimización.

El resultado de la seudonimización puede ser independiente del valor inicial (tal sería el caso de un número aleatorio generado por el responsable del tratamiento o de un apellido escogido por el interesado) o bien derivarse de los valores originales de un atributo o conjunto de atributos, como por ejemplo en el caso de funciones hash o sistemas de cifrado.

Las técnicas de seudonimización más utilizadas son las siguientes:

- Cifrado con clave secreta: En esta técnica, el poseedor de la clave puede reidentificar al interesado con suma facilidad. Para ello, le basta con descifrar el conjunto de datos, ya que este contiene los datos personales, aunque sea en forma cifrada. Si se aplican los sistemas de cifrado más avanzados, tan solo es posible descifrar los datos si se conoce la clave.
- Función hash: Se trata de una función que devuelve un resultado de tamaño fijo a partir de un valor de entrada de cualquier tamaño (esta entrada puede estar formada por un solo atributo o por un conjunto de atributos). Esta función no es reversible, es decir, no existe el riesgo de revertir el resultado, como en el caso del cifrado. Sin embargo, si se conoce el rango de los valores de entrada de la función hash, se pueden pasar estos valores por la función a fin de obtener el valor real de un registro determinado. Por ejemplo, si se aplica la función hash al número de identificación nacional para seudonimizar un conjunto de datos, dicho atributo se puede obtener simplemente ejecutando la función con todos los posibles valores de entrada y comparando los resultados con los valores del conjunto de datos. Habitualmente, las funciones hash se diseñan para poder ejecutarse de manera relativamente rápida, por lo que están sujetas a ataques de fuerza bruta[16]. También se pueden crear tablas precalculadas para lograr una reversión masiva de un gran número de valores hash.

  El uso de una función hash «con sal» (en la que se añade un valor aleatorio, conocido como «sal», al atributo al que se aplica la función hash) puede reducir la probabilidad de obtener el valor de entrada. No obstante, usando medios razonables, todavía existe la posibilidad de calcular el valor original del atributo que se oculta tras el resultado de una función hash con sal[17].
- Función con clave almacenada: Se trata de un tipo de función hash que hace uso de una clave secreta a modo de valor de entrada suplementario (lo cual la diferencia de

[16] Estos ataques consisten en probar todas las posibles entradas para crear tablas de correspondencia.
[17] Especialmente si se conoce el tipo de atributo (nombre, número de seguridad social, fecha de nacimiento, etc.). Para añadir dificultad computacional, se podría recurrir a una función hash de derivación de clave, en la que al valor computado se le aplica varias veces la función hash con poca sal.

una función hash con sal, ya que, normalmente, la sal no es secreta.) El responsable del tratamiento puede reproducir la ejecución de la función con el atributo y la clave secreta. Sin embargo, los atacantes, que no conocen la clave, lo tendrían mucho más difícil: el número de combinaciones que habría que probar sería tan grande, que convertiría este procedimiento en impracticable.

- Cifrado determinista o función hash con clave con borrado de clave: Esta técnica equivale a generar un número aleatorio a modo de seudónimo para cada atributo de la base de datos y, posteriormente, borrar la tabla de correspondencia. Esta solución[18] reduce el riesgo de vinculabilidad entre los datos personales contenidos en el conjunto de datos y los datos personales relativos a la misma persona contenidos en otro conjunto de datos en el que se usa un seudónimo diferente. Si se ejecutan los algoritmos más avanzados, el esfuerzo de cálculo que debería realizar un atacante para descifrar o reproducir la ejecución de la función sería muy grande, ya que tendría que probar cada posible clave, puesto que esta se desconoce.
- Descomposición en tokens: Esta técnica se usa típicamente en el sector financiero (aunque no exclusivamente en él) para reemplazar los números de identificación de tarjetas por valores que son de poca utilidad para los atacantes. Tiene su origen en las técnicas anteriormente mencionadas, y suele basarse en la aplicación de mecanismos de cifrado unidireccionales, o bien en la asignación, mediante una función de índice, de un número de secuencia o un número generado aleatoriamente que no derive matemáticamente de los datos originales.

4.1. Garantías

- *Singularización:* Aún es posible singularizar registros de las personas, ya que la persona queda identificada por un atributo único, que es el resultado de la función de seudonimización (es decir, el atributo seudonimizado).
- *Vinculabilidad:* La vinculabilidad entre registros que usan el mismo atributo seudonimizado para referirse a la misma persona sigue resultando sencillo. Aunque se utilizaran atributos seudonimizados diferentes para el mismo interesado, la vinculabilidad todavía sería posible a través de otros atributos. La única forma de que no haya ninguna referencia cruzada obvia entre dos conjuntos de datos que usan atributos seudonimizados diferentes es que no pueda usarse ningún otro atributo del conjunto de datos para identificar al interesado y que se haya eliminado cualquier vínculo entre el atributo original y el atributo seudonimizado (también por borrado de los datos originales).
- *Inferencia:* Se pueden llevar a cabo ataques por inferencia a la identidad real del interesado en el conjunto de datos o en diversas bases de datos que usen el mismo atributo seudonimizado para una persona, o bien en el caso de que los seudónimos sean autodescriptivos y no enmascaren adecuadamente la identidad del interesado.

4.2. Errores frecuentes

- Pensar que un conjunto de datos seudonimizado es anónimo: Con frecuencia, los responsables del tratamiento creen que basta con eliminar o remplazar uno o más atributos para convertir el conjunto de datos en anónimo. Existen muchos ejemplos que demuestran que no es así; modificar el número de identificación no basta para impedir que alguien identifique a un interesado si los cuasi identificadores siguen

[18] Depende del resto de atributos del conjunto de datos, y de si los datos originales se borran o no.

estando en el conjunto de datos, o si se pueden utilizar los valores de otros atributos para identificar a una persona. En muchos casos, identificar a una persona en un conjunto de datos seudonimizado puede ser tan sencillo como identificarla en el conjunto de datos original. Sería necesario tomar medidas adicionales para que el conjunto de datos se considerara anonimizado, entre las cuales se contarían la eliminación y generalización de atributos, el borrado de los datos originales o, al menos, la obtención un alto grado de agregación de dichos datos.

- Errores frecuentes al aplicar la seudonimización como técnica para reducir la vinculabilidad:

    - Usar la misma clave en bases de datos diferentes: La eliminación de la vinculabilidad de bases de datos diferentes depende en gran medida del uso de un algoritmo con clave y del hecho de que una única persona se corresponde con atributos seudonimizados distintos en contextos distintos. Por ello, es importante evitar usar la misma clave en bases de datos diferentes para reducir la vinculabilidad.
    - Usar claves distintas (claves «rotatorias») para cada usuario: Es tentador usar claves distintas para diferentes conjuntos de usuarios y cambiar la clave según el uso (por ejemplo: usar la misma clave para registrar 10 entradas relativas al mismo usuario). Sin embargo, si esta operación no se diseña adecuadamente, es posible que surjan patrones que reduzcan los beneficios que se persiguen. Por ejemplo, rotar la clave con arreglo a reglas específicas aplicadas a personas concretas facilitaría la vinculabilidad de las entradas correspondientes a unas personas determinadas. Además, si desaparecieran datos seudonimizados recurrentes en la base de datos al mismo tiempo que aparecen otros nuevos, esto podría ser un indicio de que ambos registros están relacionados con la misma persona física.
    - Conservar la clave: Si la clave secreta se almacena junto con los datos seudonimizados y estos se ven comprometidos, el atacante podría llegar a vincular los datos seudonimizados con el atributo original. Ocurriría lo mismo si la clave se almacenara separada de los datos, pero no de una manera segura.

4.3. Puntos débiles de la seudonimización

- *Asistencia sanitaria*

1. **Nombre, dirección, fecha de nacimiento**	**2.** **Período de prestación asistencial especial**	**3.** **Índice de masa corporal**	**6.** **Nº referencia de cohorte del estudio**
[redacted]	< 2 años	15	QA5FRD4
	> 5 años	14	2B48HFG
	< 2 años	16	RC3URPQ
	> 5 años	18	SD289K9
	< 2 años	20	5E1FL7Q

Tabla 5: Ejemplo de seudonimización con función hash (nombre, dirección, fecha de nacimiento) fácilmente reversible.

Se ha creado un conjunto de datos para estudiar la relación entre el peso de una persona y la percepción de una prestación asistencial especial. El conjunto de datos original incluye el nombre, la dirección y la fecha de nacimiento de los interesados, pero estos valores se han

borrado. El número de referencia de cohorte del estudio se ha generado a partir de los datos borrados mediante una función hash. Aunque se hayan borrado de la tabla el nombre, la dirección y la fecha de nacimiento, si se conocen estos atributos de un interesado en particular y se conociera también la función hash, sería muy fácil calcular los números de referencia de cohorte del estudio.

- *Redes sociales*

  Se ha demostrado[19] que es posible extraer información sensible de personas concretas a partir de los gráficos de redes sociales, a pesar de las técnicas de seudonimización que se aplican a estos datos. El proveedor de una red social pensaba equivocadamente que la seudonimización era una estrategia sólida para evitar la identificación, de modo que vendió datos de usuarios a otras empresas para que estas pudieran utilizarlos con fines publicitarios y de comercialización. El proveedor remplazó los nombres reales por seudónimos, pero esta medida es claramente insuficiente para anonimizar los perfiles de los usuarios, ya que las relaciones entre las distintas personas son únicas y pueden utilizarse como identificadores.

- *Localizaciones*

  Investigadores del MIT[20] analizaron recientemente un conjunto de datos seudonimizados formado por coordenadas de movilidad espacio-temporales de 1,5 millones de personas a lo largo de un período de 15 meses en un territorio con un radio de 100 km. Este análisis les permitió singularizar al 95 % de la población mediante cuatro puntos espaciales, y a más del 50 % de los interesados con apenas dos puntos espaciales (uno de esos puntos es conocido: normalmente se trata del domicilio o la oficina), con un margen muy estrecho para la protección de la privacidad, aun teniendo en cuenta que las identidades de las personas se habían seudonimizado reemplazando sus atributos verdaderos [...] por otras etiquetas.

5. Conclusiones y recomendaciones

5.1. Conclusiones

Las técnicas de desidentificación y anonimización son objeto de intenso estudio; este documento muestra de manera fehaciente que cada técnica tiene sus ventajas e inconvenientes. En la mayoría de las ocasiones, no se pueden formular recomendaciones generales sobre los parámetros que han de usarse, ya que es necesario examinar los conjuntos de datos caso por caso.

Muchas veces, un conjunto de datos anonimizado aún puede entrañar riesgos residuales para los interesados. Así, aun cuando no sea posible recuperar el registro concreto de una persona, quizá se pueda averiguar información sobre ella con ayuda de otras fuentes de información disponibles (públicas o no). Conviene subrayar que, más allá de los efectos directos que se producen sobre los interesados como consecuencia de un proceso de anonimización deficiente (molestias, pérdida de tiempo y sensación de perder el control al ser incluido en un clúster sin saberlo o sin haberlo consentido previamente), es posible que también se generen efectos

[19] A. Narayanan and V. Shmatikov, «De-anonymizing social networks», en el 30º IEEE Symposium on Security and Privacy, 2009.
[20] Y.-A. de Montjoye, C. Hidalgo, M. Verleysen y V. Blondel, «Unique in the Crowd: The privacy bounds of human mobility,» Nature, nº 1376, 2013.

secundarios indirectos debido a una anonimización deficiente si un atacante, por el hecho de tratar datos anonimizados, incluye erróneamente en su objetivo a un interesado. Estos efectos secundarios serían manifiestos sobre todo si las intenciones del atacante fueran maliciosas. Por todo ello, el Grupo de Trabajo quiere subrayar que las técnicas de anonimización pueden aportar garantías a la privacidad, pero solo si su aplicación se diseña adecuadamente, lo que significa que han de definirse con claridad los requisitos previos (el contexto) y los objetivos del proceso para obtener el grado de anonimización deseado.

5.2. Recomendaciones

- Existen limitaciones inherentes a algunas técnicas de anonimización. Los responsables del tratamiento deben ponderar seriamente estas limitaciones antes de escoger una técnica u otra para desarrollar un proceso de anonimización. Asimismo, deben atender a los fines previstos para la anonimización, como proteger la privacidad de las personas cuando se publica un conjunto de datos o permitir que se consulte algún tipo de información contenida en dicho conjunto.
- Las técnicas descritas en este documento no cumplen al cien por ciento los criterios de una anonimización efectiva, a saber: no es posible singularizar a una persona; no existe vinculabilidad entre los registros de una misma persona, y no se puede inferir información sobre una persona. No obstante, dado que cada una de estas técnicas entraña, en mayor o menor medida, alguno de estos riesgos, es imprescindible diseñar cuidadosamente la aplicación de una determinada técnica a la situación concreta de que se trate, o bien la implementación de una combinación de estas técnicas, a fin de obtener resultados más sólidos.

La tabla que se muestra a continuación ofrece un resumen de las fortalezas y debilidades de estas técnicas con relación a los tres requisitos básicos:

	¿Existe riesgo de singularización?	**¿Existe riesgo de vinculabilidad?**	**¿Existe riesgo de inferencia?**
Seudonimización	Sí	Sí	Sí
Adición de ruido	Sí	Puede que no	Puede que no
Sustitución	Sí	Sí	Puede que no
Agregación y anonimato k	No	Sí	Sí
Diversidad l	No	Sí	Puede que no
Privacidad diferencial	Puede que no	Puede que no	Puede que no
Hash/Tokens	Sí	Sí	Puede que no

Tabla 6: Fortalezas y debilidades de las técnicas analizadas.

- La solución óptima debería adoptarse caso por caso. Una solución (es decir, un proceso de anonimización integral) que cumpla estos tres criterios tendrá la solidez necesaria para impedir que la identificación de los datos se lleve a cabo mediante los medios más probables y razonables que pudiera emplear el responsable del tratamiento o cualquier tercero.
- Siempre que una posible solución no cumpla con alguno de los criterios, habrá que evaluar exhaustivamente los riesgos de identificación. Si la legislación nacional exige una valoración o autorización del proceso de anonimización por parte de las autoridades, la mencionada evaluación deberá entregarse a dichas autoridades.

Para reducir los riesgos de identificación, conviene tener en cuenta las buenas prácticas que se exponen a continuación.

Buenas prácticas de anonimización

Reglas generales:

- Publicar los datos y luego olvidarse de ellos no es una práctica fiable. Dado el riesgo residual de identificación, los responsables del tratamiento de datos deberían:
    - 1. Identificar nuevos riesgos y evaluar regularmente los riesgos residuales.
    - 2. Valorar si los controles para la identificación de riesgos son eficaces y modificarlos si fuera necesario.
    - 3. Supervisar y controlar los riesgos.
- Como parte de estos riesgos residuales, se debería considerar el potencial de identificación de la parte no anonimizada de un conjunto de datos (si es que existe), especialmente cuando se combina con la parte anonimizada, además de otras eventuales correlaciones entre atributos (p. ej., entre ubicaciones geográficas y datos de nivel de riqueza).

Elementos contextuales:

- Los objetivos que deben alcanzarse mediante el conjunto de datos anonimizado deben fijarse con toda claridad, ya que desempeñan un papel clave al determinar el riesgo de identificación.
- Esto va asociado a la valoración de la totalidad de los elementos contextuales relevantes. Por ejemplo: la naturaleza de los datos originales, los mecanismos de control que se hayan implementado (incluidas las medidas de seguridad encaminadas a restringir el acceso a las bases de datos), el tamaño de la muestra (características cuantitativas), la disponibilidad de los recursos de información públicos (en los que se basan los destinatarios) o la entrega prevista de los datos a terceros (limitada o ilimitada: p. ej., en Internet, etc.).
- No debe olvidarse la posibilidad de aparición de atacantes. Para ello, se debe valorar el atractivo que pueden tener los datos para determinados atacantes. A este respecto, la sensibilidad de la información y la naturaleza de los datos vuelven a ser factores claves.

Elementos técnicos:

- Los responsables del tratamiento deben revelar la técnica o el conjunto de técnicas de anonimización que se hayan utilizado, sobre todo si tienen la intención de publicar el conjunto de datos anonimizado.
- Deben eliminarse del conjunto de datos los atributos obvios (es decir, los raros) y los cuasi identificadores.
- Si se aplica la adición de ruido (en la aleatorización), el nivel de ruido añadido a los registros debe calcularse como una función del valor de un atributo (es decir, no debe añadirse ruido fuera de escala), del efecto que tienen en los interesados los atributos que se deben proteger y del grado de dispersión de los datos.
- Si se recurre a la privacidad diferencial (en la aleatorización), debe atenderse a la necesidad de realizar un seguimiento de las consultas a fin de detectar agresiones a la privacidad por acumulación de consultas.
- Si se utilizan técnicas de generalización, es fundamental que el responsable del tratamiento no haga uso de un único criterio de generalización, aunque sea para el mismo atributo. En otras palabras: deben seleccionarse diferentes granularidades para la localización o diferentes intervalos de tiempo. La selección de los criterios aplicables debe realizarse según la distribución de los valores de los atributos en la población dada. No todas las distribuciones se prestan a la generalización. En definitiva: esta técnica no es una

solución universal. Debe garantizarse la variabilidad en las clases de equivalencia. Por ejemplo: debe escogerse un umbral concreto en función de los elementos contextuales mencionados anteriormente (tamaño de la muestra, etc.). Si no se alcanza este umbral, debe descartarse la muestra concreta, o bien aplicarse un criterio de generalización distinto.

ANEXO
Manual de técnicas de anonimización

A.1. Introducción

El anonimato se interpreta de forma diferente en la Unión Europea. En algunos países, se entiende por tal el anonimato computacional (es decir, el correspondiente a los casos en que resulta computacionalmente difícil identificar directa o indirectamente a un interesado, aun en el caso de que el responsable del tratamiento colabore), mientras que en otros países equivale al anonimato perfecto (es decir, el que se produce cuando resulta imposible identificar directa o indirectamente a un interesado, aun en el caso de que el responsable del tratamiento colabore). Sea como fuere, en ambos casos el concepto de anonimización hace referencia al proceso por el cual se hacen anónimos determinados datos. La diferencia estriba en lo que se considera como nivel aceptable de riesgo de reidentificación.

Se pueden considerar varios usos de los datos anonimizados, desde los estudios sociales hasta los análisis estadísticos, pasando por el desarrollo de nuevos productos y servicios. En ocasiones, incluso estas actividades con finalidad general pueden tener efectos en determinados interesados, anulando la naturaleza supuestamente anónima de los datos tratados. Existen numerosos ejemplos al respecto: lanzamientos de iniciativas de comercialización con objetivos concretos, aplicación de medidas de carácter público basadas en la creación de perfiles de usuario o patrones de comportamiento y movilidad[21].

Desafortunadamente, más allá de declaraciones generales, no existe ninguna métrica lo suficientemente madura para evaluar a priori el tiempo o el esfuerzo necesarios para llevar a cabo la reidentificación tras el tratamiento, ni tampoco para seleccionar el procedimiento más adecuado, si lo que se desea es reducir la probabilidad de que una base de datos publicada haga referencia a un conjunto de interesados identificados.

El «arte de la anonimización», que es como a veces se califican estas prácticas en la literatura científica[22], es una nueva disciplina científica que aún se encuentra en sus comienzos. Aunque existen numerosas prácticas que permiten aminorar el poder de identificación de los conjuntos de datos, es importante recalcar que la mayoría de ellas no impide vincular los datos tratados con los interesados. En determinadas circunstancias, se ha constatado el éxito en la identificación de conjuntos de datos considerados anónimos; en otros casos, se han dado falsos positivos.

En general, existen dos enfoques diferentes: el primero se basa en la generalización de atributos, el segundo en la aleatorización. Adentrarnos en los detalles y las sutilezas de estas prácticas nos ayudará a comprender mejor el poder de la identificación de datos, y arrojará nueva luz sobre la noción de «datos personales».

A.2. Anonimización por aleatorización

Una de las opciones de anonimización consiste en modificar los valores reales a fin de impedir la vinculación de los datos anonimizados con los valores originales. Esto se puede conseguir haciendo uso de una extensa variedad de métodos, que van desde la adición de ruido hasta la permuta de datos (permutación). Conviene señalar que la eliminación de un

[21] Por ejemplo, el caso de TomTom en los Países Bajos (véase el ejemplo que se explica en el apartado 2.2.3).
[22] Jun Gu, Yuexian Chen, Junning Fu, Huanchun Peng, Xiaojun Ye. Synthesizing: Art of Anonymization, Database and Expert Systems Applications Lecture Notes in Computer Science –Springer- Volumen 6261, 2010, pp 385-399.

atributo es un caso extremo de aleatorización de dicho atributo, que queda completamente cubierto por el ruido.

En determinadas circunstancias, el objetivo del tratamiento global no es tanto publicar un conjunto de datos aleatorizado, sino permitir el acceso a los datos mediante consultas. En este caso, el riesgo para el interesado radica en la probabilidad de que un atacante obtenga información a partir de una serie de consultas independientes sin que el responsable del tratamiento tenga conocimiento de ello. A fin de garantizar el anonimato de las personas pertenecientes al conjunto de datos, no debería ser posible concluir que un interesado forma parte del conjunto de datos. Así, se podría romper el vínculo con cualquier tipo de conocimiento previo que pudiera poseer el atacante.

Si se añade la cantidad adecuada de ruido a la respuesta de una consulta, se puede reducir aún más el riesgo de reidentificación. Este enfoque, que la literatura denomina «privacidad diferencial»[23], se distingue de los descritos anteriormente en que proporciona a quienes publican datos un mayor control del acceso a estos, si se compara con una publicación. La adición de ruido tiene dos objetivos fundamentales: primero, proteger la intimidad de los interesados del conjunto de datos; segundo, conservar la utilidad de la información publicada. En concreto, la cantidad de ruido debe ajustarse al flujo de consultas. Si hay muchas consultas sobre personas que ofrecen respuestas demasiado exactas, aumenta la probabilidad de identificación. Hoy en día, para aplicar con éxito la aleatorización es necesario llevar a cabo una evaluación caso por caso. No existe ninguna técnica que sea cien por cien segura: existen casos de filtraciones de información en los atributos de un interesado (esté incluido o no en el conjunto de datos), incluso cuando el responsable del tratamiento ha considerado que el conjunto de datos estaba aleatorizado.

Es útil analizar ejemplos concretos a fin de aclarar los problemas potenciales de la aleatorización como herramienta de anonimización. Por ejemplo, en el contexto del acceso interactivo, las consultas que se consideran inocuas para la privacidad pueden entrañar un riesgo para los interesados. De hecho, si el atacante sabe que existe un subgrupo S de personas que pertenecen al conjunto de datos que contiene información sobre el grado de incidencia del atributo A en una población P, simplemente formulando las consultas «¿Cuántas personas en la población P poseen el atributo A?» y «¿Cuántas personas en la población P, excepto aquellas que pertenecen al subgrupo S, poseen el atributo A?» se podría determinar (por sustracción) el número de personas en S que poseen el atributo A, ya sea de forma determinista o por inferencia probabilística. En cualquier caso, la privacidad de las personas del subgrupo S podría verse seriamente amenazada, dependiendo en gran medida de la naturaleza del atributo A.

También podría ocurrir que, si un interesado no pertenece al conjunto de datos pero se conoce su relación con los datos contenidos en dicho conjunto de datos, la publicación de este último podría entrañar riesgos para su privacidad. Por ejemplo: supongamos que se sabe que «el valor del objetivo del atributo A difiere en una cantidad X del valor medio de la población». Bastaría con solicitar al responsable de la base de datos el valor medio del atributo A, que es una operación inocua para la privacidad, para que el atacante pudiera inferir con exactitud datos personales relativos a un determinado interesado.

Introducir algunas imprecisiones relativas en los valores reales de una base de datos es una operación que debe diseñarse adecuadamente. Es necesario añadir un nivel suficiente de ruido

[23] Cynthia Dwork, Differential Privacy, International Colloquium on Automata, Languages and Programming (ICALP) 2006, pp. 1–12.

para proteger la privacidad, pero no tan grande que impida preservar la utilidad de los datos. Por ejemplo: si el número de interesados que tienen un atributo muy peculiar es muy pequeño o la sensibilidad del atributo es muy alta, es mejor dar una respuesta en forma de rango de valores o en forma de frase genérica del tipo «un número pequeño de casos, posiblemente incluso cero», en lugar de proporcionar el número exacto. De esta manera, incluso en el caso de que el mecanismo de difusión de ruido se conozca previamente, se preservará la privacidad del interesado, porque persiste un cierto grado de incertidumbre. Desde el punto de vista de la utilidad, si se diseña adecuadamente esta imprecisión, los resultados seguirán siendo válidos a efectos estadísticos o de toma de decisiones.

La aleatorización de bases de datos y el acceso con privacidad diferencial plantean otras cuestiones. En primer lugar, la intensidad adecuada de distorsión puede variar significativamente según el contexto (tipo de consulta, tamaño de la población en la base de datos, naturaleza del atributo y su poder inherente de identificación), de tal modo que no existe una solución *ad omnia*. Asimismo, el contexto puede cambiar con el tiempo y, en ese caso, habría que modificar el mecanismo interactivo en consecuencia. Para calibrar el ruido es necesario hacer un seguimiento de los riesgos de privacidad acumulados que entraña para los interesados cualquier tipo de mecanismo interactivo. En ese caso, el mecanismo de acceso a los datos debería estar equipado con alertas que avisen del momento en que se alcanza el presupuesto del «coste de privacidad » y los interesados están expuestos a riesgos concretos si se lanza una nueva consulta. Así, se podrá ayudar al responsable del tratamiento a determinar el nivel de distorsión adecuado y a ir añadiendo ruido en los datos personales reales cuando corresponda.

Por otra parte, también debe considerarse el supuesto en el que se borran (o modifican) los valores de los atributos. Una solución usada frecuentemente para tratar algunos valores atípicos de atributos consiste en borrar el conjunto de datos relacionado con las personas atípicas, o bien borrar los valores atípicos. En este último caso, es importante asegurarse de que la ausencia del valor no acabe convirtiéndose en una circunstancia que permita identificar a un interesado.

Veamos ahora en qué consiste la aleatorización mediante sustitución de atributos. Una de las ideas falsas más extendidas sobre la anonimización es la de que esta equivale al cifrado o a la codificación con clave. Esta idea falsa se basa en dos suposiciones, a saber, a) que una vez que se aplica el cifrado a algunos atributos de un registro en una base de datos (p. ej., nombre, dirección, fecha de nacimiento), o si estos atributos se sustituyen con una cadena de caracteres supuestamente aleatorizada mediante una operación de codificación con clave (como una función hash con clave), entonces ese registro se ha anonimizado; y b) que la anonimización es más efectiva si la longitud de la clave es la adecuada y se utiliza un algoritmo de cifrado de última generación. Esta idea falsa está muy extendida entre los responsables del tratamiento de los datos y vale la pena aclararla, también en relación con la seudonimización y sus supuestos riesgos reducidos.

En primer lugar, hay que señalar que los objetivos de estas técnicas son radicalmente diferentes. El cifrado usado como práctica de seguridad aspira a proporcionar confidencialidad en un canal de comunicación entre varias partes identificadas (personas, dispositivos o elementos de software o hardware) a fin de evitar escuchas y la revelación no intencionada de información. La codificación con clave se corresponde con una traducción semántica de los datos con arreglo a una clave secreta. Por otra parte, el objetivo de la anonimización es impedir la identificación de personas evitando la vinculación oculta de atributos con un interesado.

Ni el cifrado ni la codificación con clave sirven en sí mismos para que un interesado no pueda ser identificado, ya que aún se puede acceder a los datos originales o deducirlos, al menos si están en manos del responsable del tratamiento. La mera implementación de una traducción semántica de datos personales (el caso de la codificación con clave) no descarta la posibilidad de revertir los datos a su estructura original, ya sea aplicando el algoritmo en sentido inverso o mediante ataques de fuerza bruta, según la naturaleza de los sistemas, o como resultado de la violación de los datos. Los sistemas de cifrado más avanzados garantizan que los datos reciben la máxima protección. En otras palabras: los datos serán ininteligibles para las entidades que desconozcan la clave de descifrado, pero esto no implica necesariamente que se haya obtenido la anonimización. Mientras se disponga de la clave o de los datos originales, no se descarta la posibilidad de identificar a un interesado, incluso en el caso de que exista un tercero de confianza que esté obligado por contrato a proporcionar un servicio seguro de depósito de claves.

Es engañoso fiarse exclusivamente de la solidez del mecanismo de cifrado como medida del grado de anonimización de un conjunto de datos, ya que existen otros muchos factores técnicos y organizativos que afectan a la seguridad global de un mecanismo de cifrado o una función hash. En la literatura se han constatado numerosos ataques con éxito que rodean completamente el algoritmo, ya sea porque se aprovechan de puntos débiles en la custodia de las claves (p. ej., un modo predeterminado menos seguro) o de otros factores humanos (p. ej., contraseñas poco seguras para la recuperación de claves). Por último, un sistema de cifrado con un tamaño de clave dado se diseña para garantizar la confidencialidad durante un período de tiempo determinado (la mayoría de las claves actuales habrán de redimensionarse en torno a 2020), mientras que un proceso de anonimización no debería estar sujeto a plazos.

Vale la pena detenerse a reflexionar sobre los límites de la aleatorización (o sustitución y eliminación) de atributos. Para ello, analizaremos diversos ejemplos desafortunados de anonimización mediante aleatorización que se han llevado a cabo en los últimos años, así como las razones que explican su ineficacia.

Un caso bien conocido de publicación de un conjunto de datos pobremente anonimizado es el del premio Netflix[24]. Si observamos un registro genérico en una base de datos donde se han aleatorizado una serie de atributos relativos a un interesado, veremos que cada registro aún se puede dividir en dos subregistros {atributos aleatorizados, atributos evidentes}, donde los atributos evidentes pueden formar cualquier combinación de datos supuestamente no personales. Con respecto al conjunto de datos del premio Netflix, se observa que cada registro se puede representar mediante un punto en un espacio multidimensional, donde cada atributo evidente es una coordenada. Mediante esta técnica, cualquier conjunto de datos puede verse como una constelación de puntos en dicho espacio multidimensional, el cual puede mostrar un alto grado de dispersión, es decir, que los puntos pueden estar muy separados los unos de los otros. De hecho, las distancias pueden ser tan largas que, tras dividir el espacio en regiones extensas, cada región contendrá únicamente un registro. Ni siquiera la adición de ruido es eficaz, porque los registros están lo suficientemente cerca como para compartir esa misma región multidimensional. Por ejemplo, en el experimento de Netflix, bastaba con conocer 8 valoraciones de películas durante un período de 14 días para hacer que los registros fueran lo suficientemente únicos. Tras añadir ruido tanto a las valoraciones como a las fechas, no se observó ninguna superposición de regiones. En otras palabras: la selección de apenas 8 películas valoradas era en sí misma una forma de identificar unívocamente las valoraciones expresadas, puesto que no eran compartidas por ningún interesado en la base de datos.

[24] Arvind Narayanan, Vitaly Shmatikov: Robust De-anonymization of Large Sparse Datasets. IEEE Symposium de IEEE on Security and Privacy, 2008, pp. 111-125.

Basándose en esta observación geométrica, los investigadores compararon el conjunto de datos supuestamente anónimo de Netflix con otra base de datos pública que contiene valoraciones de películas (IMDB), y detectaron a usuarios que habían realizado valoraciones para las mismas películas en los mismos períodos de tiempo. Dado que en la mayoría de los usuarios existía una correspondencia unívoca, se pudo importar la información auxiliar recuperada de la base de datos IMDB al conjunto de datos difundido por Netflix, lo que permitió identificar todos los registros supuestamente anonimizados.

Es importante recalcar que esto constituye una propiedad general: la parte residual de cualquier base de datos aleatorizada sigue poseyendo un alto poder de identificación, según lo rara que sea la combinación de los atributos residuales. Los responsables del tratamiento de datos no deberían olvidar nunca esta particularidad al aplicar la aleatorización como forma de alcanzar la anonimización.

Numerosos experimentos de reidentificación similares han seguido un enfoque parecido, que se basa en la proyección de dos bases de datos sobre el mismo subespacio. Se trata de un método de reidentificación muy potente que últimamente se ha aplicado en numerosas ocasiones en áreas diferentes. Por ejemplo: un experimento de identificación llevado a cabo en una red social[25], aprovechó el gráfico social de usuarios seudonimizados mediante etiquetas. En este caso, los atributos usados para la identificación eran la lista de contactos de cada usuario, ya que se ha comprobado que la probabilidad de que dos personas tengan una lista de contactos idéntica es muy baja. Basándose en esta suposición intuitiva, se descubrió que un subgráfico de las conexiones internas de un número limitado de nodos constituye una auténtica huella digital topológica que está oculta en la red, y que una gran parte de la red social en su conjunto podía identificarse después de identificar esta subred. A fin de ofrecer datos concretos sobre los resultados de un ataque similar, se mostró que, usando menos de 10 nodos (lo que puede dar origen a millones de configuraciones de subredes diferentes, donde cada una de ellas puede formar potencialmente una huella digital topológica), una red social de más de 4 millones de nodos seudonimizados y 70 millones de vínculos puede ser propensa a ataques de reidentificación, y que la intimidad de un gran número de conexiones puede verse comprometida. Debe subrayarse que este enfoque de reidentificación no está adaptado al contexto específico de las redes sociales, pero es lo suficientemente general como para adaptarse potencialmente a otras bases de datos en las que se registran las relaciones entre usuarios (p. ej., agendas de teléfono, correspondencia por correo electrónico, páginas web de citas, etc.).

Otra estrategia para identificar un registro supuestamente anónimo se basa en el análisis del estilo de escritura (estilometría)[26]. En la actualidad, se han desarrollado diversos algoritmos que permiten extraer métricas a partir del análisis de textos, incluida la frecuencia de uso de determinadas palabras, la ocurrencia de determinados patrones gramaticales y la forma de puntuación. Todas estas características pueden usarse para establecer un nexo entre un texto supuestamente anónimo y el estilo de escritura de un autor identificado. Los investigadores han determinado el estilo de escritura de más de 100 000 blogs, y hoy en día son capaces de identificar automáticamente al autor de una entrada con un margen de acierto cercano al 80 %. Se prevé que siga aumentando la precisión de esta técnica al combinarla con otras propiedades, como la localización u otros metadatos contenidos en el texto.

[25] L. Backstrom, C. Dwork, y J. M. Kleinberg. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography, Actas del 16º Congreso Internacional sobre la World Wide Web WWW'07, pp. 181-190 (2007).

[26] http://33bits.org/2012/02/20/is-writing-style-sufficient-to-deanonymize-material-posted-online/

El poder de identificación de datos a través de la semántica de un registro (es decir, de la parte residual no aleatorizada de un registro) es un asunto que merece mayor atención por parte de la comunidad científica y la industria. La reciente reversión de las identidades de donantes de ADN (2013)[27] muestra los escasos avances que se han producido desde el bien conocido incidente de AOL (2006), en el que se hizo pública una base de datos con veinte millones de palabras clave de búsqueda para más de 650 000 usuarios correspondiente a un período de 3 meses. Esto condujo a la identificación y localización de varios usuarios de AOL.

Los datos de localización forman otra familia de datos que rara vez se anonimizan y en los que simplemente se eliminan las identidades de los interesados o se cifran parcialmente algunos atributos. Es posible que los patrones de movilidad de las personas sean lo suficientemente únicos como para que la parte semántica de los datos de localización (los lugares donde el interesado se encontraba en un instante dado) pueda revelar muchas características de dicho interesado, incluso sin disponer de otros atributos[28]. Esto se ha demostrado muchas veces en estudios académicos representativos[29].

A este respecto, conviene advertir que el uso de la seudonimización no es la mejor forma de proteger adecuadamente a los interesados ante filtraciones de identidad o de atributos. Si la seudonimización se basa en la sustitución de una identidad por un código único, es muy ingenuo pensar que esta medida es una forma sólida de desidentificación, ya que no tiene en cuenta la complejidad de los métodos de identificación y los diversos contextos en que se pueden aplicar.

A.3. Anonimización por generalización

Basta un sencillo ejemplo para ilustrar el funcionamiento de la generalización de atributos.

Supongamos que el responsable del tratamiento decide publicar una simple tabla con tres tipos de datos o atributos: un número de identificación, único para cada registro, un identificador de localización, que vincula al interesado con su lugar de residencia, y un identificador de propiedad, que muestra una propiedad del interesado. Supongamos además que esta propiedad solo puede adoptar dos valores, que se indican de manera genérica como {P1, P2}:

Identificador en serie	**Identificador de la localización**	**Propiedad**
#1	Roma	P1
#2	Madrid	P1

[27] Los datos genéticos constituyen un ejemplo especialmente significativo de un conjunto datos sensibles que pueden estar en riesgo de reidentificación si el único mecanismo de anonimización que se aplica es la eliminación de las identidades de los donantes. Véase el ejemplo que aparece en el apartado 2.2.2. Véase también John Bohannon, Genealogy Databases Enable Naming of Anonymous DNA Donors, Science, Vol. 339, nº 6117 (18 de enero de 2013), p. 262.

[28] En las leyes de algunos países se ha abordado esta cuestión. Por ejemplo: en Francia, las estadísticas sobre localización que se publican se anonimizan mediante generalización y permutación. De ahí que el Instituto Nacional de Estadística y Estudios Económicos (INSEE) francés publique estadísticas que han sido generalizadas agregando la totalidad de los datos a un área de 40 000 metros cuadrados. La granularidad del conjunto de datos es suficiente para preservar la utilidad de los datos, y las permutaciones impiden los ataques de desanonimización en las áreas dispersas. En general, la agregación de esta familia de datos y su permutación ofrecen serias garantías ante la inferencia y los ataques de desanonimización (http://www.insee.fr/en/).

[29] de Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. y Blondel, V.D. Unique in the Crowd: The privacy bounds of human mobility. Nature nº 3, 1376 (2013)

#3	Londres	P2
#4	París	P1
#5	Barcelona	P1
#6	Milán	P2
#7	Nueva York	P2
#8	Berlín	P1

Tabla A1: Muestra de interesados con información sobre la localización y las propiedades P1 y P2.

Si el atacante sabe que un determinado interesado (el objetivo), que vive en Milán, está incluido en la tabla, tras examinar esta podrá averiguar que, dado que el interesado con el identificador #6 es el único que posee dicho identificador de localización, también ha de poseer la propiedad P2.

Este ejemplo elemental muestra los principales elementos de cualquier procedimiento de identificación aplicado a un conjunto de datos que ha pasado por un supuesto tratamiento de anonimización. Básicamente, tenemos un atacante que, intencionadamente o no, posee conocimientos previos sobre algunos interesados de un conjunto de datos, o sobre todos ellos. El atacante intenta vincular estos conocimientos previos con los datos del conjunto de datos publicado a fin de obtener una imagen más clara de las características de los interesados.

Para reducir la eficacia o la inmediatez de la vinculación de los datos con cualquier tipo de conocimiento previo, el responsable del tratamiento podría centrarse en el identificador de localización y sustituir la ciudad donde viven los interesados por un área más extensa, como el país. En ese caso, la tabla tendría los siguientes valores:

Identificador en serie	**Identificador de la localización**	**Propiedad**
#1	Italia	P1
#2	España	P1
#3	Reino Unido	P2
#4	Francia	P1
#5	España	P1
#6	Italia	P2
#7	Estados Unidos	P2
#8	Alemania	P1

Tabla A2: Generalización de la tabla A1 por país.

Gracias a esta nueva agregación de datos, los conocimientos previos del atacante sobre un interesado identificado (por ejemplo, «el objetivo vive en Roma y aparece en la tabla») ya no permiten extraer conclusiones claras de esta propiedad. Esto es así porque las dos personas que viven en Italia poseen distintas propiedades, en concreto, P1 y P2, respectivamente. El atacante debe asumir un 50 % de incertidumbre en relación con la propiedad de la entidad objetivo. Este sencillo ejemplo muestra el efecto que tiene la generalización en la práctica de la anonimización. De hecho, aunque este pequeño truco de generalización pueda ser eficaz para reducir a la mitad la probabilidad de identificar al objetivo italiano, no serviría para objetivos de otros lugares (p. ej., EE. UU.).

Es más, un atacante podría averiguar información sobre un objetivo de España. Si el conocimiento previo que posee es del tipo «el objetivo vive en Madrid y está en la tabla», o bien «el objetivo vive en Barcelona y está en la tabla», el atacante podría deducir con un 100 % de certidumbre que el objetivo tiene la propiedad P1. Por consiguiente, la generalización no ofrece el mismo grado de privacidad o resistencia frente a ataques por inferencia a todos los individuos de la población del conjunto de datos.

Siguiendo este razonamiento, existe la tentación de concluir que una mayor generalización podría ayudar a impedir cualquier vinculación: por ejemplo, si se generaliza por continente. En ese caso, la tabla contendría los siguientes valores:

Identificador en serie	**Identificador de la localización**	**Propiedad**
#1	Europa	P1
#2	Europa	P1
#3	Europa	P2
#4	Europa	P1
#5	Europa	P1
#6	Europa	P2
#7	América del Norte	P2
#8	Europa	P1

Tabla A3: Generalización de la tabla A1 por continente.

Con este tipo de agregación, todos los interesados que aparecen en la tabla, excepto el que vive en EE. UU., estarían protegidos ante ataques de vinculación e identificación. Cualquier conocimiento previo del tipo «el objetivo vive en Madrid y está en la tabla» o «el objetivo vive en Milán y está en la tabla» ofrecería un cierto grado de probabilidad en relación con la propiedad que poseen los interesados (P1 con una probabilidad del 71,4 %, y P2 con una probabilidad del 28,6 %), y no una vinculación directa. También conviene señalar que, con este nivel de generalización, la pérdida de información es manifiesta y extrema. La tabla no permite hallar eventuales correlaciones entre las propiedades y la localización, es decir, no se podría averiguar si un lugar puede determinar con una alta probabilidad cualquiera de las dos propiedades, dado que solo se proporcionan las denominadas distribuciones marginales, es decir, la probabilidad absoluta de las ocurrencias de P1 y P2 en el conjunto de la población (62,5 % y 37,5 %, respectivamente) y por continente (71,4 % y 28,6 %, respectivamente, en Europa, y 0 % en América del Norte).

Este ejemplo también pone de manifiesto que la práctica de la generalización afecta a la utilidad de los datos. En la actualidad, existen algunas herramientas para salvar este obstáculo anticipadamente (es decir, antes de publicar el conjunto de datos) y determinar el nivel más adecuado de generalización de los atributos, a fin de reducir los riesgos de identificación de los interesados incluidos en una tabla sin que por ello se vea demasiado afectada la utilidad de los datos publicados.

Anonimato k

El anonimato k consiste en aplicar la generalización de atributos para intentar impedir los ataques de vinculación. Esta técnica tiene su origen en un experimento de reidentificación

llevado a cabo a finales de la década de 1990. Una empresa estadounidense del sector sanitario publicó un conjunto de datos supuestamente anonimizado. La anonimización consistía en eliminar los nombres de los interesados, pero los datos aún contenían datos sanitarios y otros atributos, como el código postal (el identificador del lugar de residencia), el sexo y la fecha de nacimiento completa. Estos tres atributos {CP, sexo, fecha de nacimiento completa} también estaban contenidos en otros registros de acceso público (p. ej., el censo electoral). Por ello, un investigador pudo vincular la identidad de determinados interesados con los atributos del conjunto de datos publicado. Los conocimientos previos con los que contaba el atacante (el investigador) podrían expresarse de la siguiente forma: «Sé que el interesado aparece en el censo electoral con una combinación de tres atributos {CP, sexo, fecha de nacimiento completa} que es única. En el conjunto de datos divulgado existe un registro que contiene esta combinación». Se verificó empíricamente[30] que la gran mayoría (más del 80 %) de los interesados incluidos en el registro público utilizado en este experimento podía asociarse unívocamente a una combinación de tres atributos, lo que hacía posible la identificación. Por lo tanto, en este caso los datos no se habían anonimizado de manera adecuada.

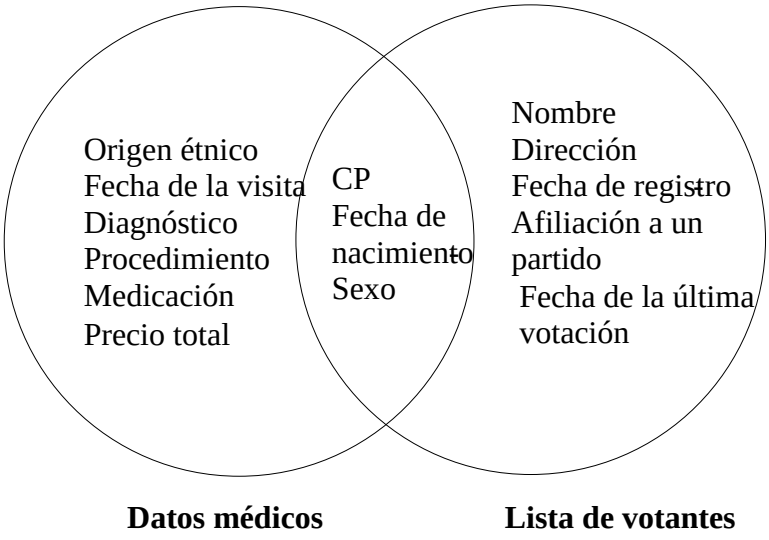

Figura A1: Reidentificación mediante vinculación de datos.

Para reducir la eficacia de ataques de vinculación similares, los responsables del tratamiento deberían examinar el conjunto de datos y agrupar aquellos atributos que pudieran razonablemente ser usados por un atacante para vincular la tabla publicada con otra fuente auxiliar. Cada grupo debería incluir al menos *k* combinaciones idénticas de atributos sometidos a generalización. Es decir, debería representar una clase de equivalencia de atributos. Posteriormente, los conjuntos de datos deberían publicarse solo tras dividirse en estos grupos homogéneos. Los atributos a los que se aplica la generalización se conocen en la literatura como «cuasi identificadores», ya que la revelación de la información que contienen implica la identificación inmediata de los interesados.

Se han llevado a cabo numerosos experimentos de identificación para mostrar la debilidad de tablas con anonimato k defectuosamente diseñadas. Esto puede ocurrir, por ejemplo, cuando el resto de los atributos de una clase de equivalencia son idénticos (como ocurre con la clase

[30] L. Sweeney. Weaving Technology and Policy Together to Maintain Confidentiality. Journal of Law, Medicine &Ethics, 25, nº 2 y 3 (1997), pp. 98-110.

de equivalencia de los interesados españoles en el ejemplo de la tabla A2) o su distribución sufre un serio desequilibrio con una alta prevalencia de un atributo en concreto. Esta técnica también es débil cuando el número de registros en una clase de equivalencia es muy bajo. En estos dos casos mencionados, se puede producir una inferencia probabilística. También puede darse esta debilidad en la técnica cuando no existe ninguna diferencia «semántica» entre los atributos evidentes de las clases de equivalencia (p. ej., la medida cuantitativa de estos atributos puede ser, en la práctica, diferente, pero muy próxima al valor real; o bien pueden pertenecer a un rango de atributos semánticamente similares: p. ej., el mismo rango de riesgo crediticio, o la misma familia de patologías). En todos estos casos, desde el conjunto de datos aún podría filtrarse una gran cantidad de información sobre los interesados que podría utilizarse en los ataques de vinculación[31]. Aquí conviene señalar que, siempre que los datos estén dispersos (por ejemplo, existen pocas ocurrencias de una propiedad concreta en una área geográfica) y que una primera agregación no pueda agrupar los datos con un número suficiente de ocurrencias de propiedades diferentes (por ejemplo, se sigue localizando un número reducido de ocurrencias de algunas pocas propiedades en un área geográfica), es necesario llevar a cabo una agregación ulterior de los atributos a fin de obtener la anonimización deseada.

Diversidad l

Basándose en estas observaciones, a lo largo de los años se han propuesto variantes del anonimato k y se han ido estableciendo criterios de diseño que permiten mejorar la implantación de la anonimización mediante generalización. El objetivo último es reducir los riesgos de los ataques de vinculación. Estas variantes se basan en las propiedades probabilísticas de los conjuntos de datos. En concreto, añaden la restricción de que cada atributo en una clase de equivalencia debe aparecer al menos *l* veces. De esta forma, el atacante siempre tendrá que afrontar una incertidumbre significativa en los atributos, incluso en el caso de que disponga de conocimientos previos sobre un determinado interesado. Esto equivale a decir que un conjunto de datos (o partición) debe poseer un número mínimo de ocurrencias de una propiedad seleccionada. Este truco puede mitigar el riesgo de reidentificación, que es el objetivo de la anonimización mediante diversidad l. Se muestra un ejemplo de esta técnica en las tablas A4 (datos originales) y A5 (resultados del tratamiento). Como resulta evidente, si los valores del identificador de la localización y de la edad de las personas (tabla A4) se diseñan adecuadamente, la generalización de atributos puede resultar en un sustancial incremento de la incertidumbre con respecto a los atributos reales de todos los interesados. Por ejemplo: si el atacante supiera que un interesado pertenece a la primera clase de equivalencia, no podría determinar a ciencia cierta si una persona posee la propiedad X, Y o Z, ya que existe al menos un registro en esa clase (y en todas las clases) con esa propiedad.

Número de serie	Identificador de la localización	Edad	Propiedad
1	111	38	X
2	122	39	X
3	122	31	Y

[31] Cabe señalar que las correlaciones también pueden determinarse una vez que se hayan agrupado los registros de datos por atributos. Cuando el responsable del tratamiento sabe qué tipos de correlaciones desea verificar, puede seleccionar los atributos más relevantes. Por ejemplo, los resultados de los estudios llevados a cabo por PEW no están sujetos a ataques por inferencia de grano fino, y siguen siendo muy útiles para hallar correlaciones entre la demografía y los intereses (http://www.pewinternet.org/Reports/2013/Anonymity-online.aspx).

4	111	33	Y
5	231	60	Z
6	231	65	X
7	233	57	Y
8	233	59	Y
9	111	41	Z
10	111	47	Z
11	122	46	Z
12	122	45	Z

Tabla A4: Personas agrupadas por localización, edad y las tres propiedades X, Y y Z.

Número de serie	Identificador de la localización	Edad	Propiedad
1	11*	<50	X
4	11*	<50	Y
9	11*	<50	Z
10	11*	<50	Z
5	23*	>50	Z
6	23*	>50	X
7	23*	>50	Y
8	23*	>50	Y
2	12*	<50	X
3	12*	<50	Y
11	12*	<50	Z
12	12*	<50	Z

Tabla A5: Ejemplo de una versión de la tabla 4 con diversidad 1.

Proximidad t

La proximidad t es una técnica que permite salvar los obstáculos que surgen cuando los atributos de una partición están distribuidos de manera no uniforme o pertenecen a un rango de valores o significados semánticos muy estrecho. Se trata de otra mejora de la anonimización por generalización que consiste en reorganizar los datos para obtener clases de equivalencia que reflejan al máximo posible la distribución inicial de los atributos en el conjunto de datos original. Para ello, se sigue un procedimiento que consta básicamente de dos pasos. La tabla A6 es la base de datos original, que incluye registros evidentes de interesados, agrupados por localización, edad, salario y dos familias de propiedades semánticamente similares, respectivamente, (X1, X2, X3) y (Y1, Y2, Y3) (p. ej.: clases similares de riesgo crediticio y enfermedades parecidas). Primero, se aplica a la tabla la *diversidad l* con *l*=1 (tabla A7), agrupando los registros en clases de equivalencia semánticamente similares, con lo que se obtiene una anonimización muy débil. Después, se trata para alcanzar una proximidad t (tabla A8) y una mayor variabilidad en cada partición. De hecho, en este segundo paso, cada clase de equivalencia incluirá registros de las dos familias de propiedades. Conviene subrayar que tanto el identificador de localización como la edad tienen granularidades diferentes en los diversos pasos del proceso. Esto significa que puede que cada atributo requiera criterios de generalización diferentes para obtener la anonimización deseada. Esto, a su vez, exige que los responsables del tratamiento de los datos lleven a cabo un diseño específico y dediquen el tiempo necesario para la computación.

Número de serie	Identificador de la localización	Edad	Salario	Propiedad
1	1127	29	30K	X1
2	1112	22	32K	X2
3	1128	27	35K	X3
4	1215	43	50K	X2
5	1219	52	120K	Y1
6	1216	47	60K	Y2
7	1115	30	55K	Y2
8	1123	36	100K	Y3
9	1117	32	110K	X3

Tabla A6: Personas agrupadas por localización, edad, salario y dos familias de propiedades.

Número de serie	Identificador de la localización	Edad	Salario	Propiedad
1	11**	2*	30K	X1
2	11**	2*	32K	X2
3	11**	2*	35K	X3
4	121*	>40	50K	X2
5	121*	>40	120K	Y1
6	121*	>40	60K	Y2
7	11**	3*	55K	Y2
8	11**	3*	100K	Y3
9	11**	3*	110K	X3

Tabla A7: Versión de la tabla A6 con diversidad *l*.

Número en serie	Identificador de la localización	Edad	Salario	Propiedad
1	112*	<40	30K	X1
3	112*	<40	35K	X3
8	112*	<40	100K	Y3
4	121*	>40	50K	X2
5	121*	>40	120K	Y1
6	121*	>40	60K	Y2
2	111*	<40	32K	X2
7	111*	<40	55K	Y2
9	111*	<40	110K	X3

Tabla A8: Versión de la tabla A6 con proximidad *t*.

Es importante recalcar que el objetivo de generalizar los atributos de los interesados, haciendo uso de estas estrategias tan elaboradas, en ocasiones tan solo puede alcanzarse para un número muy reducido de registros y no para la totalidad de los mismos. Las buenas prácticas deberían garantizar que cada clase de equivalencia contenga varias personas y que no exista la posibilidad de que se produzca un ataque por inferencia. En cualquier caso, este enfoque exige un examen exhaustivo de los datos disponibles por parte de los responsables del tratamiento de datos, así como una evaluación combinatoria de las diversas alternativas (por ejemplo, diferentes rangos de amplitudes o distintas granularidades de la localización y la edad). En definitiva: la anonimización por generalización no puede ser el resultado de un

primer intento burdo por parte de los responsables del tratamiento de datos de sustituir los valores analíticos de los atributos de un registro por rangos. Es necesario adoptar estrategias cuantitativas más concretas, como la evaluación de la entropía de los atributos en cada partición, o la medición de la distancia entre las distribuciones de atributos originales y la distribución en cada clase de equivalencia.