UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería Informática

TRABAJO FIN DE GRADO

DESARROLLO BASADO EN MODELOS DEL REGLAMENTO GDPR

Guillermo López Lázaro
Tutora: María Elena Gómez Martínez
Ponente: Juan De Lara Jaramillo

JULIO 2020

DESARROLLO BASADO EN MODELOS DEL REGLAMENTO GDPR

AUTOR: Guillermo López Lázaro
TUTORA: María Elena Gómez Martínez

Dpto. INGENIERÍA INFORMÁTICA
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Julio de 2020

Resumen

Este Trabajo Fin de Grado propone crear una representación basada en modelos del *"General Data Protection Regulation"* (GDPR). Dicho reglamento europeo facilita a los ciudadanos el poder ejercer sus derechos sobre su información de carácter personal sin que exista ningún tipo de riesgo en el tratamiento de ésta. Los modelos a partir de los cuales se representará el reglamento podrán ser utilizados en procesos software, tales como el Proceso Unificado Software o metodologías ágiles. Para la obtención de estos, se ha llevado a cabo un desarrollo basado en MDE (*Model-Driven Engineering*) usando como tecnología EMF (*Eclipse Modeling Framework*), en el que primeramente se ha analizado en detalle el reglamento GDPR, y después se ha representado.

En el análisis realizado, se ha obtenido toda la información acerca de los distintos artículos que rigen el reglamento, desde las entidades participantes hasta las relaciones entre las mismas, así como las diferentes actividades de las que formarán parte. Para realizar dicho análisis, lo primero que se ha hecho es leer todo el reglamento con detenimiento, empezando por el preludio y siguiendo con los numerosos artículos que lo componen. Seguidamente, se ha estudiado cada artículo extrayendo todos los conceptos clave correspondientes anteriormente mencionados. Finalmente, una vez obtenida toda la información necesaria, se ha generado el modelo en cuestión.

Todo lo comentado con anterioridad, se ha realizado con el objetivo de conseguir un modelo del reglamento GDPR aplicable a cualquier contexto real y específico. En nuestro caso, al final del documento que nos concierne, se ha aplicado con éxito a modo de ejemplo a una situación concreta asociada con la gestión de un sistema de préstamo de libros en una biblioteca.

Palabras clave

GDPR, datos personales, MDE, modelo, EMF, tratamiento, Reglamento.

Abstract

This Bachelor Thesis dissertation aims to propose a model-based representation of the *"General Data Protection Regulation"* (GDPR), which allows the citizens to exercise their personal information rights without the possibility of suffering risks at that process. That representation will be done through models, which will be built by making an interpretation of the European GDPR (General Data Protection Regulation) regulation. That models will be able to be used in software processes (for example: Unified Software Process). With this purpose, it has been done a MDE (Model-driven engineering) development using EMF (Eclipse Modeling Framework), analysing GDPR regulation in detail first, and representing it later.

In that analysing process, we have obtained the whole information related to the GDPR articles, starting from the participant entities, going through the relationships between them, and focusing in the different activities that they will take part of. To make that analysis, the first thing that we have made is reading the whole regulation in detail, starting from the prelude and then, continuing with the numerous articles. After that, we have studied every article deducing the whole key concepts mentioned before. Finally, at the time that we have the information we wanted, it has been generated the model.

The process we have described, it has been done with the goal of obtain a GDPR model that can be used in several real and specific situations. In our case, at the end of this document, the model has been successfully applied to a concrete context related to the book lending service present in a library.

Keywords

GDPR, personal data, MDE, model, EMF, processing, Regulation.

Agradecimientos

Me gustaría agradecer a todas aquellas personas que me han apoyado a lo largo de mi vida todo lo que han hecho por mí, porque sin ellos este TFG no habría sido posible.

En primer lugar, a mis padres, ya que siempre estuvieron ahí, tanto para lo bueno como para lo malo, y me enseñaron a no rendirme nunca. Sin su educación no estaría hoy donde estoy. En segundo lugar, a mi tutora del TFG, Elena, por su dedicación y el esfuerzo realizado para que todo esto saliera adelante. Siempre estuvo disponible cuando fue necesario. En tercer lugar, a mi perro, Doby, que siempre tuvo la paciencia para esperar un ratito más a que yo terminase de hacer TFG para sacarle a la calle. Sin la alegría y desconexión que me ha proporcionado esto no habría sido posible. Y, por último, y no por ello menos importante, a mi pareja, sin su apoyo e inspiración, no habría llegado hasta aquí.

Gracias a todos.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

1 Introducción

1.1 Motivación

En la actualidad, vivimos en una sociedad muy avanzada y plenamente tecnológica, en la que el contacto entre las diferentes organizaciones y personas es continuo. Como consecuencia, nuestros datos personales están constantemente en circulación. Además, cada día el volumen de datos es mayor, lo que hace que estos sean cada vez más complicados de manejar.

Por esta razón, es necesario que se lleve y regule un control exhaustivo de la utilización y el transporte de todos los datos personales. Dicho control, deberá garantizar dos cosas: el derecho a la protección de los datos de carácter personal y el derecho a la libre circulación. A raíz de esta necesidad, la Comisión Europea propuso el reglamento GDPR (*General Data Protection Regulation*) [1], que viene a sustituir a la antigua Directiva 95/46/CE [2]. Esta directiva, debido a las características de la sociedad actual, no conseguía abarcar todas las necesidades estructurales, ya que, por ejemplo, no se encargaba de controlar los datos de carácter personal que circulaban por las redes sociales, ni tampoco los de gran parte de las nuevas tecnologías que han ido apareciendo desde su publicación en 1995. Esto, provocaba un uso fraudulento de la información, generándose por ejemplo un gran mercado en la venta de datos. Como consecuencia, y con el objetivo de proteger al interesado contra este tipo de acciones, el Parlamento Europeo, junto con el Consejo de la Unión Europea, elaboraron el nuevo reglamento GDPR, el cual entró en vigor en mayo de 2018. Dicho reglamento se adaptó a la legislación española en la Ley Orgánica de Protección de Datos Personales y garantía de los Derechos Digitales (LOPDP) [3], vigente desde diciembre de 2018.

Debido al surgimiento de este nuevo reglamento, tan importante en la materia de la protección de datos, aparece la necesidad de conseguir aplicar y manejar dicha legislación de la manera más eficaz y correcta posible. En la actualidad, la tarea de vigilar el cumplimiento de la ley siempre es llevada a cabo por la figura de un experto en la materia (más adelante veremos que a esta figura se le conoce como delegado de protección de datos o DPD), quien, tras realizar un análisis profundo y detallado de la organización o sistema que está evaluando, elabora un informe en el cual explica qué partes del reglamento se están cumpliendo y cuáles no. Esto tiene un problema, y es que siempre se está realizando el análisis *a posteriori*, es decir, una vez se ha construido toda la infraestructura del sistema. Por ejemplo, si disponemos de una aplicación de gestión de citas médicas, este análisis se estaría realizando una vez la aplicación es plenamente funcional e incluso se halle en el mercado. Esto conlleva, además de un gran problema de seguridad, que la organización evaluada en cuestión tenga que volver a recorrer todas las fases de desarrollo de nuevo para conseguir cumplir todo aquello que no hacía antes.

Por ello, para solucionar este problema es necesario garantizar la protección de los datos personales de las personas físicas de una manera más eficiente, además de evitar procesos de desarrollo inapropiados y facilitar el recorrido de estos. Una de las soluciones que se proponen, en base a lo anteriormente comentado, es la realización de modelos del reglamento, los cuales nos servirán para representar de manera más abstracta todo lo que dicta el nuevo mandato. Estos modelos, se realizarán al comienzo del ciclo de desarrollo, de tal manera que, al aplicarlos, ya en la fase de diseño se conocerán cuáles son los requisitos legales que se deben cumplir, y, por lo tanto, podremos desde un principio adaptar nuestro

diseño y posterior desarrollo a ellos. Es en este contexto y ámbito donde nace el presente Trabajo Fin de Grado.

1.2 Objetivos

Este TFG tiene varios objetivos. En primer lugar, se deberá llevar a cabo una interpretación clara y concisa del reglamento GDPR, es decir, habrá que leer y estudiar todas y cada una de las partes que lo componen, alcanzando así los conocimientos necesarios que nos permitan acometer el resto de los objetivos.

En segundo lugar, deberemos realizar un análisis completo y detallado de los artículos que componen el reglamento, identificando a lo largo del proceso los conceptos clave, así como las relaciones entre los mismos.

Una vez hayamos realizado el análisis, tendremos que ser capaces de conseguir representar toda aquella información extraída en un modelo, es decir, deberemos modelar el reglamento GDPR. Esta representación tendrá que ser lo más clara y detallada posible, ya que otro de los objetivos será lograr que ese modelo sea aplicable a cualquier contexto real y específico. Además, y en base a esto último, una de las tareas consistirá en aplicar el modelo obtenido a una situación concreta.

1.3 Organización de la memoria

La memoria de este Trabajo de Fin de Grado consta de los siguientes capítulos:

En el Capítulo 2, "Estado del arte*"*, se analiza brevemente la situación actual en el ámbito de la interpretación del reglamento GDPR, así como de las propuestas hasta la fecha llevadas a cabo para facilitar su aplicación.

En el Capítulo 3, "Marco teórico y tecnológico", contaremos cuál es el medio teórico en el que nos moveremos en cuanto a reglamentación de la protección de datos, así como cuales han sido los medios tecnológicos usados para la realización del TFG.

En el Capítulo 4, "Modelado del GDPR", se explicará al comienzo cuál ha sido la metodología seguida para la obtención del modelo y cómo se ha llevado a cabo el análisis del reglamento GDPR. Una vez hecho esto, se irá analizando en detalle el modelo obtenido.

En el Capítulo 5, "Integración, pruebas y resultados", aplicaremos el modelo obtenido a un contexto real específico y comprobaremos su eficacia.

En el Capítulo 6, "Conclusiones y trabajo futuro", se explicarán las conclusiones a las cuales hemos llegado tras el desarrollo del TFG, así como se hablará de cuáles pueden ser las implementaciones futuras que pueden realizarse en esta materia y trabajo.

2 Estado del arte

El objetivo de esta sección es explicar la situación actual por la que pasa la protección de datos y los intentos llevados a cabo para modelar el reglamento GDPR (*General Data Protection Regulation)* [1]. Para ello, hablaremos del contexto en el que nos encontramos, así como del estudio de la materia que se ha realizado hasta la fecha.

Con el fin de conseguir obtener una imagen representativa y manejable de lo que es el reglamento GDPR, y poder trabajar con él, se han llevado a cabo numerosos estudios para conseguir modelarlo. A continuación, analizaremos algunos de los artículos de estudio más importantes.

Torre et al. [4] destacan la importancia de adquirir una serie de modelos que permitan automatizar la comprobación del cumplimiento del reglamento, es decir, saber en cada momento, en base a una situación específica y un contexto dado, cuando el reglamento GDPR se está cumpliendo con éxito y por ello respetando todos y cada uno de sus artículos. Según los autores, para las empresas se ha convertido en una verdadera complicación el hecho de tener que comprobar el cumplimiento a cada momento del reglamento GDPR, ya que, además de ser de gran extensión, carecen de modelos o cualquier elemento de abstracción que facilite la tarea, por lo que deben revisar manualmente dicho cumplimiento. Esta tarea, se realiza bajo la atenta mirada de los organismos del gobierno, que pueden llegar a poner multas de varios millones de euros si no se cumple con lo que dicta el reglamento. Por tanto, proponen la posibilidad de crear dos tipos de modelos: genéricos, los cuales servirán como primera toma general de contacto, y específicos, que permitirán aplicar el reglamento en situaciones concretas y definidas. Además, explican cuáles serían los 4 pasos que seguir para poder comprobar el cumplimiento del reglamento:

1. Construir una representación/clasificación genérica, es decir, crear el modelo genérico.
2. Adaptar dicho modelo a una representación específica dentro de un contexto (modelo específico).
3. Generar representaciones estructuradas del modelo específico en las cuales se pueda aplicar el chequeo automático del cumplimiento del reglamento (instancias).
4. Comprobar el cumplimiento del reglamento.

Cabe destacar, y como explicaremos más adelante, que el presente TFG se centra en los pasos 1 y 2, debido a la extensión del GDPR. En el paso 1, será donde crearemos nuestro modelo del reglamento GDPR, para más tarde en el paso 2, aplicar el modelo creado a una situación específica de la vida real.

Por otro lado, Rabinia et al. [5] concluyen sobre la enorme dificultad que supone modelar un reglamento, proceso tras el cual se suelen obtener modelos muy complejos y de difícil comprensión debido a la cantidad de artículos que lo componen y a la complejidad de estos y de la materia tratada. Los autores proponen la utilización de un *framework,* llamado "Formal Legal_GRL Framework" (*FLG*), asociado a una metodología que ayuda a resolver las complejidades de los modelos y facilita la automatización en la creación de estos. Dicha metodología se basa en la creencia de que las representaciones visuales y naturales son más fáciles de entender y usar. En el documento se enumeran 3 fases por las que pasa todo modelado mediante el *FLG*:

1. Fase A: extraer los requisitos legales mediante el procedimiento propio de FLG.
2. Fase B: guardar los resultados obtenidos en una base de datos.
3. Fase C: crear el modelo.

En [5] se centran principalmente en describir la fase A, la cual, como hemos mencionado con anterioridad, se basa en extraer los requerimientos legales del reglamento y aplicarles cierto tratamiento, todo ello con el fin de reducir la complejidad del modelo. Este proceso de tratamiento se puede resumir en 3 pasos:

1. Extraer los requerimientos y dividirlos en 3 tipos: obligaciones, prohibiciones y permisos (derechos). Con ello, al tenerlo todo bien estructurado, se busca simplificar la estructura del modelo final.
2. Formalizar los requerimientos en expresiones lógicas, a través de las cuales podamos representar las distintas relaciones entre entidades y los diferentes tipos de requerimientos.
3. Verificar y comprobar cuales son los casos de posible no cumplimiento del reglamento que pudieran llegar a darse y tener claro cómo se obtienen.

En comparación con este TFG, podemos observar como el trabajo de Rabinia et al. también busca estructurar de alguna manera el reglamento. En su caso, ellos dividen el contenido en tres grupos, mientras que nosotros, como veremos más adelante, decidimos dividirlo en clases según los conceptos clave que vayamos encontrando durante el análisis del reglamento.

Por otra parte, Blanco-Lainé et al. [6] destacan la importancia que ha supuesto el reglamento actual GDPR en lo que a las empresas se refiere, ya que, resulta complicado entender los requerimientos legales que dicta la norma, y se debe tener sumo cuidado a la hora de vigilar el cumplimiento de estos, ya que cualquier tipo de error puede impactar a todos los niveles de la empresa. Los autores intentan facilitar este proceso. Para ello, proponen usar modelos EAM (*Enterprise Architecture Model*, modelos de la arquitectura de la empresa) para representar el reglamento GDPR. Esta aproximación consigue que podamos relacionar de una forma directa la arquitectura de una empresa con la que arquitectura que conforma el reglamento GDPR, y, por consecuencia, ayudar al cumplimiento del reglamento. Además, realizan una pequeña representación del reglamento GDPR utilizando el software ArchiMate [7], el cual está diseñado específicamente para representar arquitecturas de empresas y modelarlas. Como vemos, este último trabajo también se apoya en la idea de realizar representaciones visuales y esquemáticas a través de modelos con el objetivo de lograr una mejor interpretación del reglamento.

En lo que respecta a nuestro TFG, de igual manera que los trabajos anteriormente comentados, utilizamos representaciones visuales estructuradas del reglamento GDPR con el objetivo de conseguir una mejor interpretación de este, reducir su complejidad, y con ello realizar posteriormente un modelo aplicable a situaciones reales y específicas. En las siguientes secciones analizaremos el proceso seguido y el resultado obtenido.

3 Marco teórico y tecnológico

El objetivo de este apartado es explicar brevemente el marco de referencia del proyecto y las tecnologías utilizadas para su desarrollo.

3.1 GDPR y LOPDP

En este TFG, el marco teórico gira en torno a dos regulaciones: el reglamento europeo GDPR [1], y la ley española LOPDP [3] (*"Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales"*).

El reglamento europeo GDPR ha nacido para sustituir a la antigua directiva 95/46/CE [2], la cual, debido a las características actuales de la sociedad, se había quedado obsoleta. Este nuevo reglamento, basado en la protección de los datos de carácter personal de los interesados, tiene como objetivo proporcionar al interesado un control más exhaustivo de sus datos personales, todo ello adaptado a la sociedad tecnológica en la que vivimos. Además, al tratarse de una ley genérica y conocida por todos, se pretende facilitar a las organizaciones y empresas el cumplimiento de los derechos del interesado. El reglamento, elaborado por el Parlamento Europeo y el Consejo Europeo, está dividido en varias secciones según la temática, y consta de 99 artículos.

Por su parte, la ley LOPDP surge a raíz del nacimiento del reglamento GDPR, ya que esta es la adaptación española del mencionado reglamento europeo. Por ello, compartirá objetivos con respecto al GDPR, con la principal diferencia en el ámbito de aplicación de esta (la ley LOPDP solo aplica en España). En este caso, la regulación española cuenta con 97 artículos, divididos de nuevo en varias categorías según la temática.

En nuestro caso, como buscamos encontrar un modelo aplicable a cualquier tipo de situación, nos centraremos únicamente en el reglamento GDPR, ya que aplica a nivel general en todo el territorio europeo, mientras que la ley LOPDP es una adaptación específica para el territorio español, y por lo tanto de igual manera cada país de la Unión Europea contará con su respectiva regulación.

3.2 Ingeniería basada en Modelos

Un modelo, como indican Montenegro et al. [8], *"es una abstracción de la realidad"*, la cual será representada de manera mucho más simplificada. Si nos adentramos en un nivel más, tenemos la definición de metamodelo, que, según los autores anteriormente mencionados, *"es un modelo que describe un Lenguaje de Modelado (LM), con el que se describen otros modelos"*, entendiéndose como lenguaje de modelado el lenguaje utilizado para el diseño del metamodelo. Un ejemplo de lenguaje de modelado es UML [9]. Además, es importante señalar un tercer concepto: los lenguajes de dominio específico o DSL. Estos lenguajes son los que obtenemos tras la realización de nuestros metamodelos, y son aplicables a otros contextos de ámbito similar al estudiado en el metamodelo. A partir de este momento, será importante saber distinguir entre todos estos conceptos. En este apartado, nos centraremos en los modelos, y será en el subapartado 3.2.1 donde hablaremos del metamodelo y el lenguaje DSL obtenido.

En lo que respecta a la representación del GDPR realizada, es importante destacar que se ha desarrollado inspirándonos en la ingeniería basada en modelos (*Model-Driven Engineering*,

MDE). Dicha aproximación se basa en una metodología de desarrollo del software centrada en la creación de modelos como representación abstracta de problemas concretos [10]. Estos modelos constan de todo tipo de características con el fin de obtener una imagen representativa del problema: entidades, atributos, reglas, relaciones entre entidades, etc. Gracias al nivel de abstracción que se alcanza con esta tecnología podemos representar y simplificar en gran medida problemas o estructuras muy complejas, como es el caso del reglamento GDPR.

Las ventajas que aporta este tipo de modelado son muy diversas. Por un lado, gracias a las tecnologías que permiten trabajar con MDE, conseguimos realizar diseños muy intuitivos y de fácil comprensión, ya que este tipo de tecnologías se centran en ofrecer al usuario la posibilidad de obtener resultados muy visuales y esquemáticos. Además, estos modelos generados tienen un componente muy alto de portabilidad, ya que pueden ser utilizados, de la manera adecuada, para cualquier otro tipo de problemas de similar ámbito, es decir, una vez finalizado el proceso, tendremos la capacidad de realizar una implementación o aplicación de nuestro modelo a una situación específica de la vida real. Por último, se automatiza mucho la generación de código que se realiza a posteriori, ya que en casi todas las tecnologías que usemos para modelar bastará con seleccionar la opción correspondiente para que se genere el código de manera totalmente automática. Además, si realizamos cualquier tipo de cambio, solo tendremos que volver a seleccionar dicha opción para verlo reflejado.

3.2.1 Eclipse y EMF

Para la realización del presente TFG, en base a la propuesta de mi tutora, se ha utilizado un entorno de desarrollo integrado llamado *Eclipse* [11]. Dicho entorno está compuesto de un conjunto de herramientas de programación de código abierto, a través de los cuáles se pueden realizar todo tipo de productos. Además, se nos proporciona la posibilidad de añadir nueva funcionalidad propia a la herramienta (*plugins*[1]). Hay que señalar que, además de *Eclipse*, existen otras herramientas para MDE, como son por ejemplo el caso de *Visual Paradigm* [12] o *Enterprise Architect* [13].

En concreto, para la obtención del metamodelo, se ha utilizado un *framework* específico llamado *Eclipse Modeling Framework* (EMF) [14], el cual está formado por un conjunto de *plugins* que nos permiten modelar un metamodelo, para después generar código basado en él, el cual pueda ser utilizado en situaciones específicas, es decir, sirva para aplicar dicho modelo. En este caso, nuestro lenguaje de dominio específico DSL será el metamodelo del reglamento que hemos obtenido, el cual podremos aplicar a otros contextos de similar ámbito. Podemos diferenciar dos partes importantes dentro del modelado en EMF:

[1] Un plugin es aquella aplicación que, en un programa informático, añade una funcionalidad adicional o una nueva característica al software. [18]

- ***ecore***: es la parte que contiene la información de las clases definidas en el metamodelo. En ella podemos añadir fácilmente desde nuevas entidades, así como atributos, o relaciones entre los mismos. La Figura 1 muestra un extracto del ecore que define el GDPR.

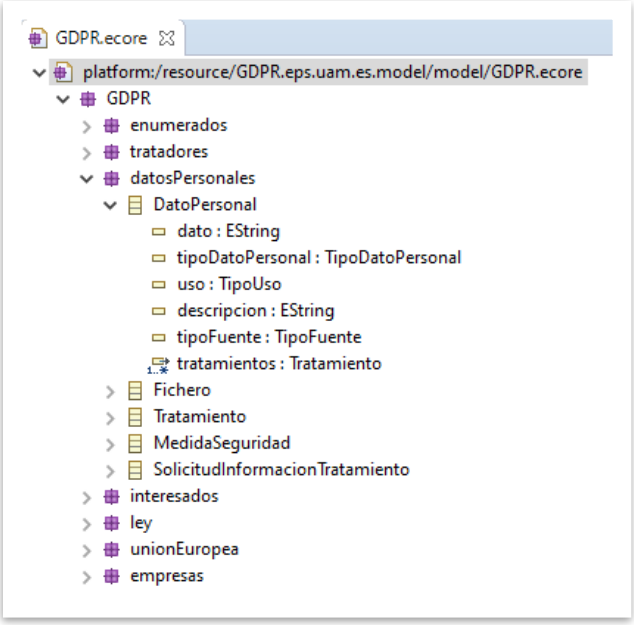

Figura 1: Parte ecore del framework EMF

- ***aird:*** es la parte donde podremos visualizar las representaciones gráficas que hayamos generado de los distintos "paquetes" del modelo. En el entorno de Eclipse encontraremos esta funcionalidad a partir de la parte de *ecore*.

4 Modelado del GDPR

4.1 Metodología

La finalidad de esta sección es explicar el proceso y metodologías llevadas a cabo para la obtención del modelo del GDPR basado en MDE.

Para empezar, fue necesaria una breve lectura acerca de cuál era el estado del arte de la protección de datos [4], así como de sus leyes y derechos más importantes. Seguidamente, se realizó una lectura más en profundidad del reglamento GDPR que nos acontece [1], prestando especial interés al contexto y motivo de la creación de éste. En concreto, se leyeron los 173 apartados que comprenden el preludio a los artículos.

Una vez se tuvo una idea clara del reglamento en cuestión, se fue analizando manualmente artículo a artículo. Dicho análisis se basó en los siguientes pasos:

1. Lectura en detalle del artículo: donde se presta especial atención a la redacción de éste.

2. Análisis sobre la necesidad de incluir el artículo en el modelo: donde se estudia el papel que tendría el artículo y se decidió sobre su inclusión. En caso de considerarse fuera del ámbito del modelo el artículo quedó descartado.

3. Extracción de los términos clave: donde se señalan qué conceptos clave son necesarios para la correcta construcción del metamodelo, es decir, cuáles serán los elementos protagonistas que nos permitirán controlar el comportamiento de los diferentes procesos llevados a cabo en la protección de datos. Esta extracción se realizó de manera completamente manual, aunque hay que señalar que existen herramientas automáticas para ello, como es el caso de *Atlas.ti* [15].

4. Clasificación de términos clave: donde se catalogan los diferentes conceptos clave obtenidos en tres categorías: clases, que representarán a las entidades participantes en el reglamento GDPR así como las diferentes estructuras de información creadas; atributos, que reflejaran las características y cualidades propias de las clases anteriormente extraídas; y métodos, donde se detallarán las distintas acciones y funciones que las entidades y figuras del tratamiento de datos personales desempeñarán.

5. Establecimiento de las relaciones entre las clases: donde se detallan todos los enlaces existentes entre las diferentes clases.

6. Realización del diagrama de clases EMF: donde se transforman todas las anotaciones y observaciones previas en el metamodelo en cuestión, todo ello a través de un diagrama EMF. El *framework* EMF, como hemos comentado con anterioridad en el punto 3, además de proporcionarnos la capacidad de realizar el metamodelado, nos permite generar código a partir de dicha construcción.

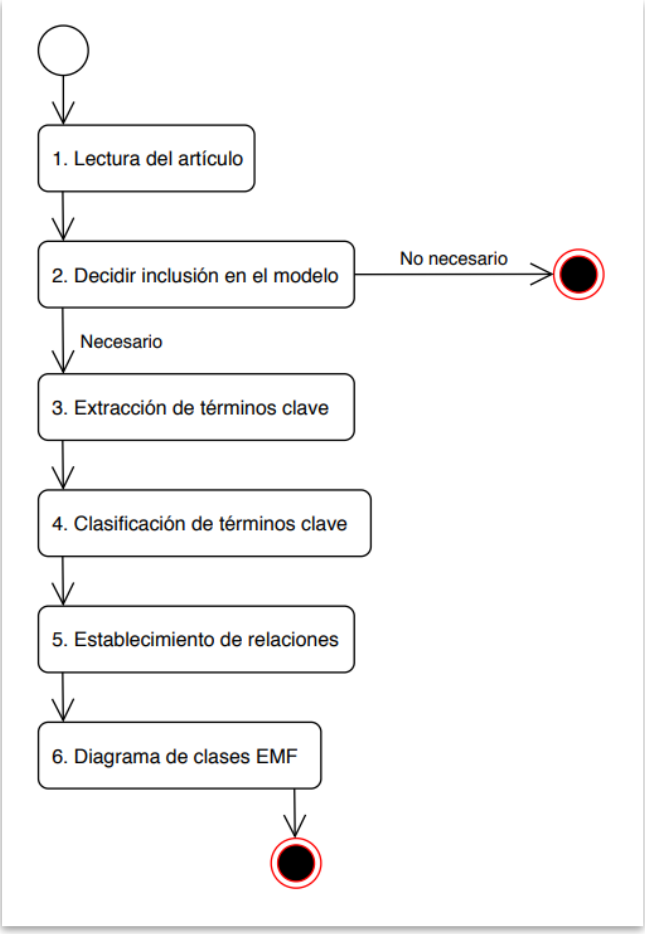

Figura 2: Diagrama de actividad de los pasos para el análisis de un artículo

A continuación, se procederá a explicar con un ejemplo sencillo la metodología anteriormente descrita. El apartado 6 del Art. 4 del GDPR establece los siguiente:

"6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;"

Los 6 pasos a realizar para el análisis del artículo son los siguientes:

1. El primer paso será leer con detenimiento el artículo, comprendiendo cada parte de este y fijándonos en su redacción. Como vemos, en este caso se trata de una definición, por lo que deberemos centrarnos en entender el concepto explicado.

2. Seguidamente, se estudia si el artículo en cuestión debe ser analizado en detalle para su inclusión de una manera u otra en el metamodelo. Como podemos ver, al ser una definición de una entidad, y dada su importancia, decidiremos seguir con el proceso de análisis.

3. El tercer paso será extraer los posibles conceptos clave que nos encontremos, es decir, cuáles serán los elementos protagonistas que nos permitirán controlar el comportamiento de los diferentes procesos llevados a cabo en la protección de datos.

En este caso, como partes clave existirán: un fichero, datos personales y el tipo de fichero.

4. A continuación, nos tocará clasificar los términos clave extraídos con anterioridad. Por un lado, al ser un artículo de definiciones, cada definición será una nueva clase que crear, por lo que contaremos con la clase "Fichero". Es importante también darnos cuenta de que será necesario que una segunda clase "DatoPersonal" exista, debido a que un fichero será "*todo conjunto estructurado de datos personales…*". Seguidamente, vemos que podemos establecer como atributo (característica) el tipo de fichero (centralizado, descentralizado o repartido). Esto se hará mediante la creación de un enumerado ("TipoFichero"). Por otra parte, esta vez no contamos con ningún método.

5. Seguidamente, habrá que identificar las relaciones entre clases. Cabe destacar que la clase fichero tendrá una relación de composición con la clase "DatoPersonal" previamente creada.

6. A continuación, tendremos que representar en un diagrama de clases EMF todos los datos recogidos. La Figura 3 ilustra el ejemplo:

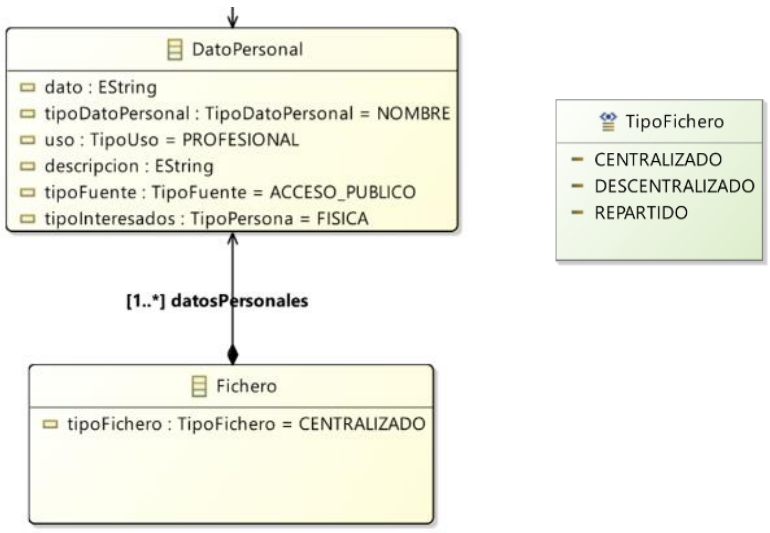

Figura 3: Diagrama EMF de ejemplo

Como se ha comentado, la clase *DatoPersonal* ha sido creada previamente en otro artículo.

4.2 Representación del GDPR

El objetivo de este apartado es describir el modelo obtenido tras el análisis del GDPR que se ha llevado a cabo. Para ello, detallaremos los paquetes obtenidos en el diagrama EMF. Dichos paquetes, como hemos comentado con anterioridad, están formados por clases, los cuales a su vez están formados por atributos y métodos. Todos ellos en su totalidad, junto con las relaciones asociadas entre clases, forman el análisis realizado propiamente dicho.

Existen 7 paquetes (ver Figura 4): *Ley*, donde se define el reglamento GDPR como tal; *Interesados*, que muestra todo lo referido a las personas físicas cuyos datos personales son tratados; *DatosPersonales*, orientado como indica su nombre a contener toda la información de carácter personal de los interesados, así como la forma de tratarla; *Tratadores*, destinado a representar a las personas que se encargan de tratar la información; *UnionEuropea*, donde se describen todos los organismos involucrados en el GDPR; *Empresas*, que señala la estructuración de las empresas implicadas en el tratamiento; y, por último, *Enumerados*, que contiene todos los tipos necesarios para algunos de los atributos de las clases.

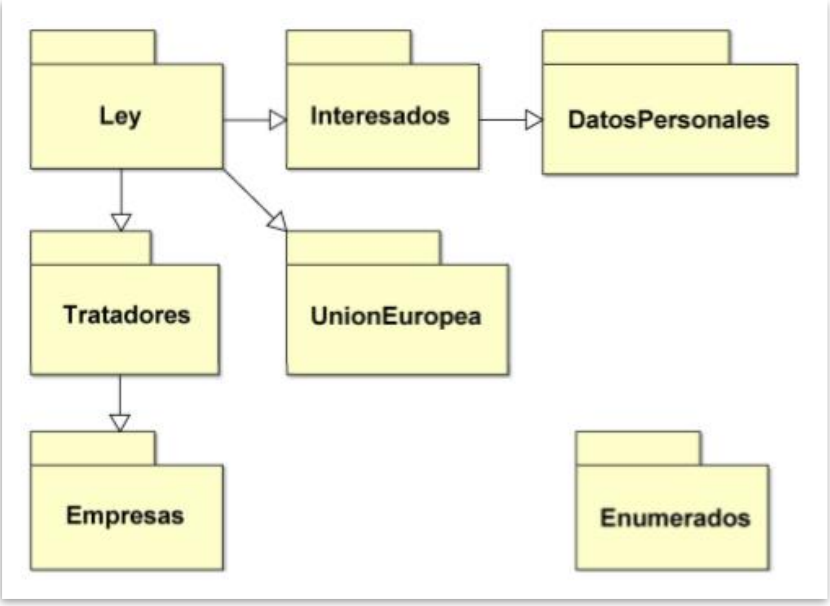

Figura 4: Diagrama representativo de los distintos paquetes

A continuación, detallaremos los paquetes, excepto el paquete *Enumerados*, el cual se detallado en el Anexo A. Hay que destacar que en el análisis de los paquetes no se muestran los métodos, incluidas sus representaciones gráficas, por brevedad. La explicación de los métodos y los diagramas completos se mostrarán en el Anexo B. Además, remarcar que la información extraída es la relacionada propiamente con el tratamiento de los datos personales, por tanto, habrá artículos que no aporten información relevante para nuestro análisis, ya que no estén relacionados directamente con el tratamiento.

4.2.1 Paquete Ley

El paquete `Ley` se encarga de representar todo aquello relacionado con el reglamento GDPR, y nos permite estructurar el propio reglamento, es decir, no se ha obtenido a partir de la definición de ningún artículo de ésta. Las clases que lo componen son las siguientes, ver Figura 5:

- Clase `GDPR`: hace referencia al reglamento, el cual está formado por una lista de artículos. En este caso, nuestra clase solo cuenta con un atributo:
  - `articulos`:[2] referencia a una lista de artículos de tipo `Articulo`.

- Clase `Articulo`: define la estructura de un artículo. Como hemos mencionado anteriormente, esta clase será la componente única y fundamental de la clase GDPR. Esto se debe puramente al carácter y composición de un reglamento. Los atributos y relaciones que componen a un artículo son:
  - `numero`: indica el número de artículo del reglamento GDPR.
  - `titulo`: contiene el título del artículo.
  - `descripcion`: almacena el texto del artículo en sí.

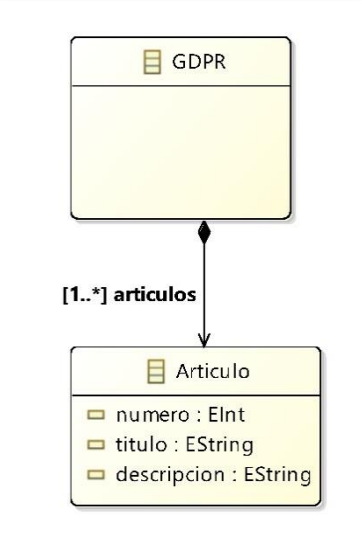

Figura 5: Paquete Ley

4.2.2 Paquete Interesados

En este paquete se muestran todas las entidades relacionadas con las personas sobre las que se aplica un tratamiento de datos, es decir, las denominadas como personas físicas o interesados. Las clases que lo componen son las siguientes, ver Figura 6:

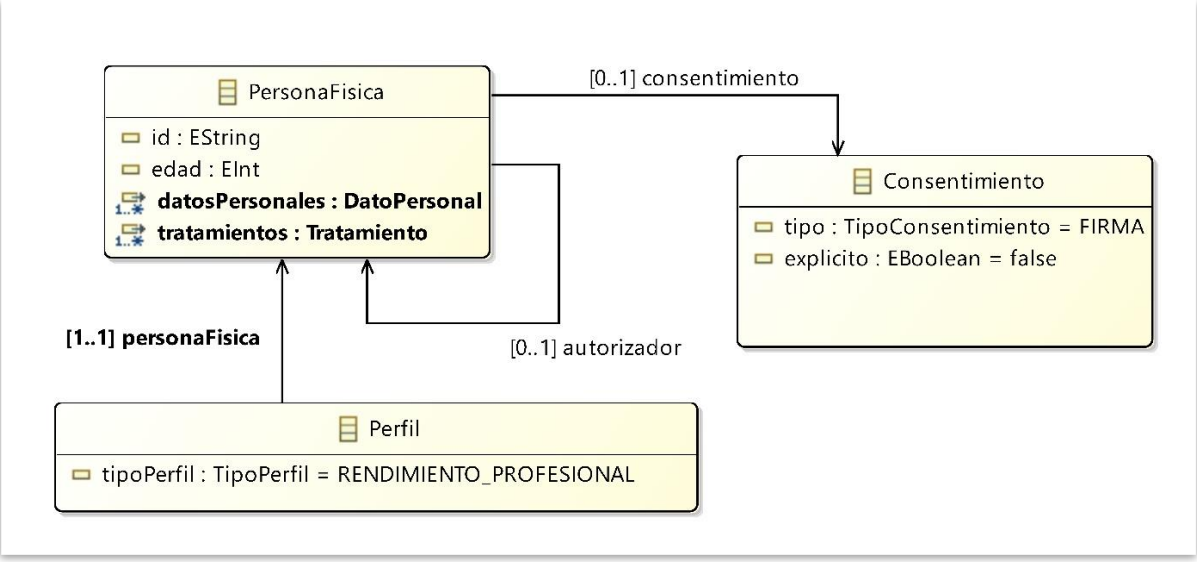

Figura 6: Paquete *Interesados*

- Clase `PersonaFisica`: esta clase es la encargada de almacenar todo lo relacionado con los interesados (personas físicas). Como se puede leer en el Art.1.1 del GDPR: *"El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales […]"),* deberemos tener una clase que haga referencia a todas aquellas personas a las

[2] El nombre de las clases, atributos y métodos no ha tenido en cuenta la ortografía del idioma español.

que se les vaya a aplicar un tratamiento de datos de carácter personal. Los atributos y relaciones de esta clase son los siguientes:

- `id`: sirve como identificador único de las personas físicas en el sistema. Su presencia, pese a no estar motivada por ningún artículo, resulta imprescindible, ya que se basa fundamentalmente en la necesidad identificar de manera inequívoca al individuo, pero sin usar ninguno de sus datos personales.
- `edad`: edad de la persona física. Según el Art.8.1 ("*Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, […]"*), cuando una persona física sea menor de 16 años se necesitará el consentimiento de un tutor o autorizador para permitir el tratamiento. Este parámetro no se almacenará en los datos personales ya que dichos datos solo recogerán los aspectos relacionados con el tratamiento en sí, y en este caso es necesario conocer previo tratamiento la edad del interesado.
- `datosPersonales`: lista de datos personales de la persona física. Como hemos visto con anterioridad en el Art.1.1, los interesados tendrán una serie de datos asociados a su persona. Estos datos serán los que se utilicen en los tratamientos y serán de tipo `DatoPersonal`, clase que se detalla en la Sección 4.2.3.
- `tratamientos`: lista de los tratamientos asociados a la persona física. Un tratamiento, como veremos más adelante en la sección 4.2.3, tendrá toda la información acerca de cómo se van a tratar los datos personales del interesado. Este atributo nace a raíz de la necesidad estructural de tener recogidos los tratamientos de cada interesado en una estructura. A lo largo de todo el reglamento GDPR, y como veremos más adelante, se hace referencia a las diversas acciones que se pueden ejecutar sobre los distintos tratamientos, desde solicitar la información de estos hasta pedir la supresión de estos, y ello no sería posible sin que la persona física conociese y tuviese accesos a esos tratamientos mencionados. Los tratamientos son de tipo `Tratamiento` (ver sección 4.2.3).
- `autorizador`: persona física que autoriza a otra a recibir tratamiento. En el Art.8.1 se habla de la necesidad de la existencia de una persona física que autorice el tratamiento de datos cuando la persona física es menor de 16 años.
- `consentimiento`: atributo de tipo `Consentimiento` que nos permite saber si la persona física ha dado o no su consentimiento para el tratamiento de los datos personales. La necesidad de la creación de este atributo está recogida en el Art.4.11 del reglamento GDPR: *"«consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;"*.

- Clase `Perfil`: clase encargada de almacenar un perfil de datos de la persona física en base a los tratamientos realizados. Como indica el Art.4.4 (*"«elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física […]"*), se crearán perfiles de los interesados con todos los datos que se hayan podido recoger. Es por ello por lo que surge la necesidad de recoger dichos

perfiles en una estructura específica, en este caso nuestra clase `Perfil`. Los atributos y relaciones de esta clase son los siguientes:

- `personaFisica`: persona a la que pertenece el perfil.
- `tipoPerfil`: tipo de perfil del que se dispone. Como indica el Art.4.4 del GDPR, *"[…]en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;"*, los perfiles podrán ser de diversos tipos. Como hemos comentado con anterioridad, los enumerados se representarán en el anexo A.

- Clase `Consentimiento`: clase destinada a recoger el consentimiento proporcionado por la persona física para autorizar el tratamiento correspondiente. Como hemos comentado con anterioridad, en el Art.4.11 se muestra la definición a través de la cual se ha tomado la decisión de crear la clase. Los atributos y relaciones de esta clase son los siguientes:
  - `tipo`: tipo de consentimiento dado. La creación de este no se rige directamente por el reglamento, pero es claro que el consentimiento se podrá manifestar de varias maneras, desde a través de una simple firma, hasta vía huella dactilar.
  - `explicito`: atributo que puede tomar un valor verdadero o falso dependiendo de si el consentimiento ha sido explícito por parte de la persona física o no. La creación de este atributo nace de la necesidad en varios puntos del reglamento GDPR de conocer dicho carácter acerca del consentimiento. Es el caso del Art.9.2.a, donde se explica que las personas físicas no podrán recibir tratamiento de sus datos si al realizarse se revelan datos de origen político o religioso. En dicho artículo, si el consentimiento proporcionado es explícito *("[…] el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados […]"*), el tratamiento anteriormente mencionado será válido.

4.2.3 Paquete DatosPersonales

En este paquete se muestran todas las entidades relacionadas con los datos personales sobre los que se aplica un tratamiento. Las clases que lo componen son las siguientes, ver Figura 7:

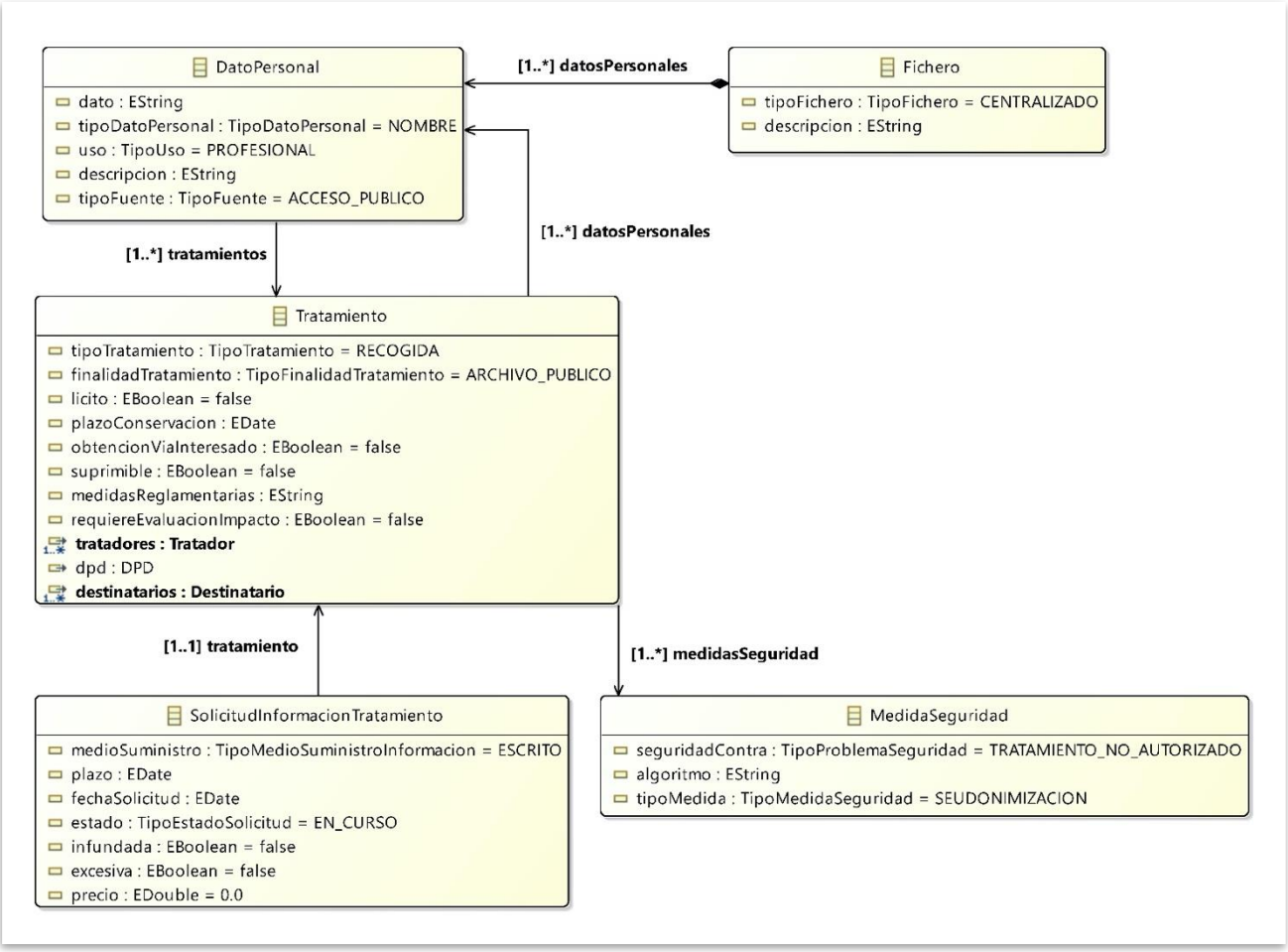

Figura 7: Paquete DatosPersonales

- Clase `DatoPersonal`: clase encargada de almacenar un dato personal de una persona física. Como apunta el Art.1.1 (*"El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales […]"*), los interesados tendrán asociados una serie de datos personales a su persona. Los atributos y relaciones de esta clase son los siguientes:
  - `dato`: atributo que contiene el nombre específico del dato personal. El origen de éste reside en la necesidad instintiva de nombrar de alguna manera a cada dato personal.
  - `tipoDatoPersonal`: tipo de dato personal. Según el Art.4.1, existen distintas categorías de datos: *"[…] toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"*.
  - `uso`: tipo de utilización del dato personal. En el Art.2.2, se indican las excepciones en las cuales el GDPR no se podrá aplicar. Una de las excepciones (Art.2.2.c) dependerá del tipo de uso de los datos personales que se esté llevando a cabo, ya que no será aplicable el reglamento si los datos

personales son de uso doméstico o personal. La excepción indicada es la siguiente: *"efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;"*.

- descripcion: atributo que almacena una descripción más detallada del dato personal. De la misma forma que el atributo `dato`, no tiene su origen en ningún artículo en concreto, pero su uso se considera necesario ya que el nombre del dato podría no ser lo suficientemente descriptivo y llevar a confusiones.
- tipoFuente: tipo de fuente de la que proceden los datos personales. Según el Art.14.2.f, deberemos distinguir entre fuente de acceso público o privado: *"[…] si proceden de fuentes de acceso público;"*.
- tratamientos: lista de los tratamientos asociados al dato personal. Este atributo nace a raíz de la necesidad estructural y lógica de tener recogidos los tratamientos de cada dato personal en una estructura. Los tratamientos, como veremos a continuación, son de tipo `Tratamiento`.

- Clase `Fichero`: clase que contiene un conjunto de datos personales de manera estructurada. Según el Art.4.6 (*"«fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;"*), los datos personales se organizarán en ficheros de acuerdo con una serie de parámetros. Los atributos y relaciones de esta clase son los siguientes:
  - datosPersonales: datos personales que contiene el fichero.
  - tipoFichero: tipo del fichero. Como hemos visto en el Art.4.6, el fichero podrá ser de tres tipos: centralizado, descentralizado o repartido. Todas estas opciones se contemplan en el enumerado correspondiente `TipoFichero` que puede verse en el anexo A.
  - descripción: útil y breve descripción del fichero.

- Clase `Tratamiento`: clase encargada de almacenar toda la información asociada a un tratamiento. Según el Art.4, denominado *"Definiciones"*, deberemos tener una entidad que recoja todo lo relacionado con el tratamiento en sí de los datos personales del interesado. En concreto, en el Art.4.2 tendremos lo siguiente: *"«tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales […]"*. Además, a lo largo de todo el reglamento GDPR vamos viendo como en sucesivas ocasiones se hace referencia a aspectos propios del tratamiento que se realiza, por lo que resulta imprescindible almacenar todos ellos de forma estructurada. Esta clase tiene los siguientes atributos y relaciones:
  - tipoTratamiento: atributo que especifica el tipo de tratamiento. Los diferentes tipos existentes se pueden ver referenciados en el Art.4.2 anteriormente mencionado: *"[…] como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"*.
  - finalidadTratamiento: cada tratamiento será realizado con una finalidad. En el Art.5.1.b podemos comprobar dicha afirmación: *"[…] el tratamiento ulterior de los datos personales con fines de archivo en interés*

público, fines de investigación científica e histórica o fines estadísticos". Los detalles se muestran en el Anexo A.

- `licito`: atributo que permite saber si el tratamiento realizado es lícito o no. Según el Art.6.1 (*"El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: […]"*), será importante analizar una serie de condiciones que nos permitan conocer si el tratamiento cumple con el reglamento o si por el contrario se vulnera alguna ordenanza. El resultado de dicho análisis se recogerá en este atributo.
- `plazoConservacion`: según el Art.5.1.e, los tratamientos tendrán un plazo de conservación asociado a los datos personales que contienen, es decir, los tratadores solo podrán conservar dicha información hasta cierta cantidad de tiempo: *"sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);"*.
- `obtencionViaInteresado`: atributo que nos indicará si los datos personales del tratamiento han sido obtenidos vía interesado o no. Según el Art.13.1: *"Cuando se obtengan de un interesado datos personales relativos a él […]"*, por tanto, se da una lista con la información a transmitir en el caso de que los datos se obtengan a partir del interesado. Como veremos en la sección 4.2.4, la figura del responsable de tratamiento será la encargada de transmitir la información correspondiente.
- `suprimible`: atributo en el que podemos ver si el tratamiento podrá ser eliminado. Como indica el Art.17.1, *"El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:"*, es decir, en base a una situación concreta, el tratamiento podrá ser suprimido y dejará de tener efecto.
- `medidasReglamentarias`: según el Art.24.1, *"[…] el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento […]"*.
- `requiereEvaluacionImpacto`: atributo que nos indica si el tratamiento necesita una evaluación de impacto, es decir, si requiere que se analice en profundidad ante el riesgo de que se pongan en peligro los derechos y libertades de las personas físicas. Este atributo nace a partir del Art.35.3, donde se expone lo siguiente: *"La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de: […]"*.
- `tratadores`: lista de personas u organizaciones que intervienen a lo largo del proceso de un tratamiento. Dichos tratadores, serán de tipo `Tratador`, clase detallada en la sección 4.2.4. Además, es importante señalar que este atributo se ha implementado por razones estructurales, ya que la persona física tendrá asociados sus tratamientos, pero no así los tratadores, por lo que accederá a ellos a través de este atributo.
- `DPD`: delegado de protección de datos. Todo tratamiento de datos debe tener un DPD, el cual será el encargado de controlar y supervisar si se está llevando a cabo de manera correcta el tratamiento de los datos personales de los interesados. En el Art.13.1.b podemos observar la necesidad de incluirlo en

nuestra clase `Tratamiento`: *"los datos de contacto del delegado de protección de datos, en su caso;"*. La clase `DPD` será explicada en la Sección 4.2.4.

- `destinatarios`: entidades encargadas de recibir datos personales de forma indirecta. Como establece el Art.13.1.e, los destinatarios serán uno de los datos que el interesado deba recibir cuando se vaya a realizar un tratamiento de sus datos personales: *"los destinatarios o las categorías de destinatarios de los datos personales, en su caso;"*.
- `medidasSeguridad`: según el Art.32.1, el tratamiento deberá recibir una serie de medidas de seguridad: *"[…] el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo […]"*. Estas medidas de seguridad serán descritas más adelante en esta sección cuando hablemos de la clase `MedidaSeguridad`.
- `datosPersonales`: son los datos personales propiamente dichos a los que hace referencia el tratamiento.

Respecto a los métodos obtenidos, pese a que hacen referencia a cuestiones y acciones propias de los interesados, se encuentran en este paquete. Esto es debido a que, estructuralmente, se aplican sobre el tratamiento, por lo que se ha decidido ubicarlos en esta clase.

- Clase `SolicitudInformacionTratamiento`: clase que contiene toda la información que recibirá el interesado cuando éste la solicite (en base a los métodos de la clase `Tratamiento` detallados en el anexo B). Se ha decidido implementar debido a la necesidad de tener dicha información recogida de manera estructurada, ya que en sucesivos artículos se hacía referencia a información específica de la solicitud mencionada. Los atributos y relaciones de esta clase son los siguientes:
  - `medioSuministro`: medio a través del cual será suministrada la información al interesado. Según el Art.12.1, la información podrá ser transmitida de forma escrita, vía medios electrónicos o de forma verbal: *"[…] La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios."*.
  - `plazo`: como se ha visto en el Art.5.1.e, los tratamientos tendrán un determinado plazo asociado al que tendrán que adaptarse.
  - `fechaSolicitud`: como establece el Art.12.3 (*"El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. […]"*), para aplicar la norma de transmisión de información del tratamiento será necesario conocer la fecha en la cual el interesado realizó dicha solicitud.
  - `estado`: estado en el que se encuentra la solicitud de información del tratamiento. Además de poder estar en curso, según el Art.12.3 (*"[…] Dicho plazo podrá prorrogarse […]"*) y el Art.12.4 (*"Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación […]"*), la solicitud podrá encontrarse

prorrogada o ser cancelada. Este estado se contemplará en el enumerado `TipoEstadoSolicitud` (Anexo A).

- `infundada`: atributo que indica si la solicitud es infundada, es decir, si carece o no de fundamento. En el Art.12.5 podemos observar la necesidad de la creación de este: *"[…] Cuando las solicitudes sean manifiestamente infundadas o excesivas […]"*.
- `excesiva`: atributo que indica si la solicitud es excesiva, es decir, si se han realizado ya o no demasiadas solicitudes como para considerar la que nos concierne como excesiva. Según el Art.12.5 una solicitud puede ser excesiva si….
- `precio`: coste de la solicitud. En un principio las solicitudes serán gratuitas, no obstante, el responsable podrá cobrar cierta cantidad en base a lo recogido en el Art.12.5.a: *"cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada […]"*. Esto se aplicará, como indica el Art.12.5, en los casos en los que las solicitudes sean infundadas o excesivas.
- `tratamiento`: tratamiento asociado a la solicitud. Gracias a la inclusión de este atributo el interesado podrá acceder a la información propia del tratamiento.

- Clase `MedidaSeguridad`: clase encargada de almacenar toda la información asociada a las medidas de seguridad en la clase `Tratamiento`. Los atributos y relaciones de esta clase son los siguientes:
  - `seguridadContra`: tipo de problema de seguridad que puede surgir en un tratamiento. Según el Art.5.1.f, se deberá garantizar la seguridad contra varios problemas: *"tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, […]"*.
  - `algoritmo`: como su nombre indica, las medidas de seguridad implementadas contarán con un algoritmo de aplicación. Esto, pese a no venir indicado como tal en el reglamento, será introducido como atributo en base a una necesidad lógica y estructural, ya que toda medida de seguridad, especialmente si se trata de un contexto tecnológico, sigue un algoritmo.
  - `tipoMedida`: tipo de medida de seguridad aplicada. En el Art.32.1, se comenta la necesidad de distinguir entre varios tipos de medidas de seguridad: *"el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: […]"*. En los subapartados siguientes de dicho artículo, se enumeran los tipos de medidas.

4.2.4 Paquete Tratadores

En este paquete se muestran todas las entidades relacionadas con las personas u organizaciones que ejercen el tratamiento. La Figura 8 muestra las clases que lo componen:

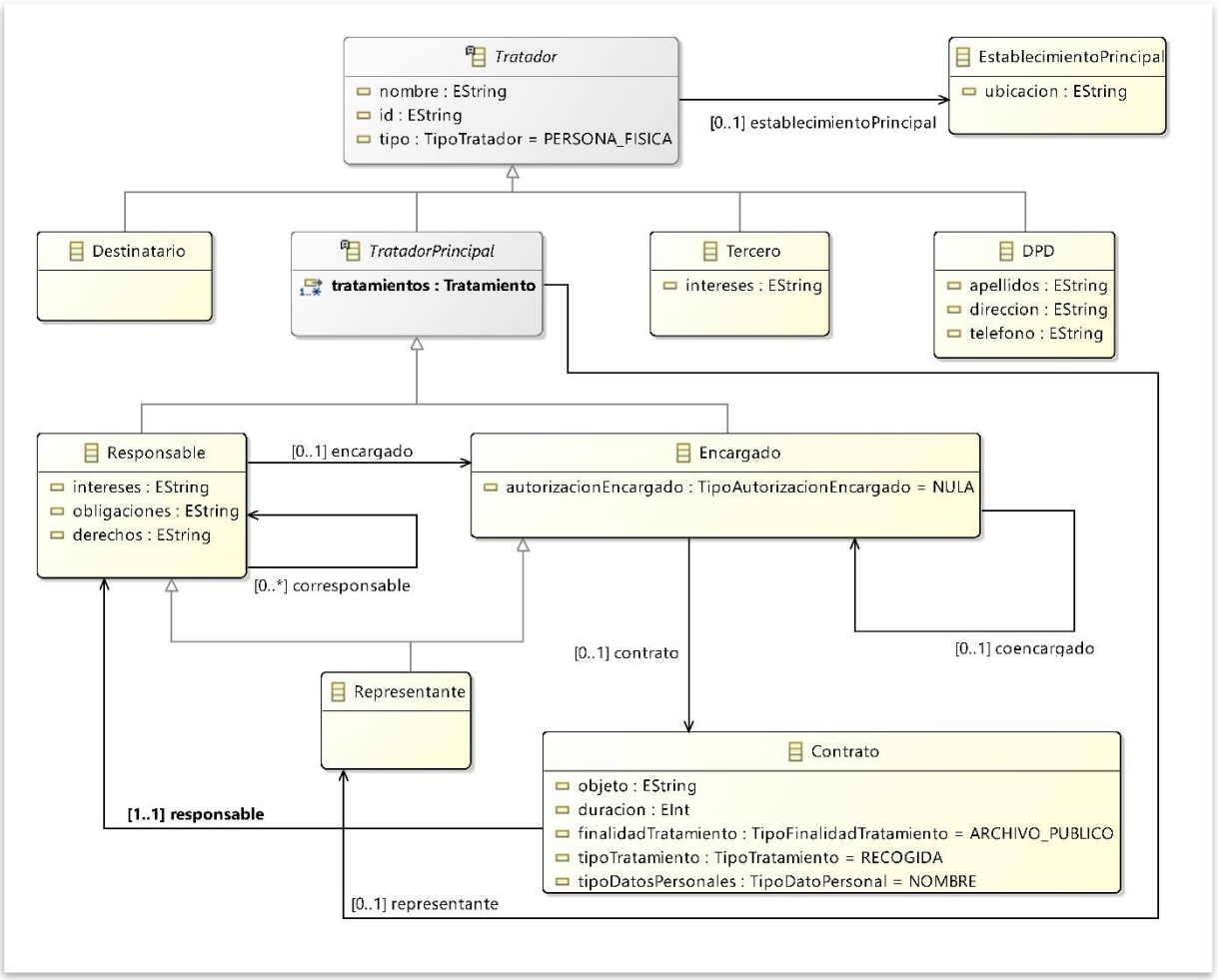

Figura 8: Paquete *Tratadores*

- Clase `Tratador`: clase encargada de aglutinar a todas y cada una de las personas u organizaciones que participan, de una manera u otra, en el tratamiento de los datos personales. A lo largo de todo el GDPR, surgen varias entidades participantes en un tratamiento de datos. Ejemplos de ello son los responsables del tratamiento (Art.24: *"Responsabilidad del responsable del tratamiento"*) o los encargados de este (Art.28: *"Encargado del tratamiento"*). Dichas entidades, serán detalladas en esta sección más adelante. Los atributos y relaciones de nuestra clase `Tratador` son:
  - `nombre`: nombre del tratador. Según los artículos Art.30.1.a y Art.30.2.a, los tratadores tendrán un nombre asociado. Es el caso, por ejemplo, de los responsables. El Art.30.1.a dicta lo siguiente: *"el nombre y los datos de contacto del responsable […]"*. De igual manera sucederá con el resto de las figuras reconocidas como tratadores, ya sean encargados del tratamiento o desempeñen cualquier otro tipo de función.
  - `id`: sirve como identificador único de los tratadores dentro de una aplicación. Su presencia, pese a no estar motivada por ningún artículo, resulta imprescindible, y se basa fundamentalmente en la necesidad de identificar dentro del sistema a un tratador de manera inequívoca.
  - `tipo`: tipo de tratador. Tal y como indica el Art.4 en varios subapartados, el tratador podrá ser de distinta índole. Así, por ejemplo, siguiendo con el ejemplo del responsable, el Art.4.7 dice lo siguiente: *"«responsable del*

tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento;".

- `establecimientoPrincipal`: lugar de trabajo donde el tratador desempeñará las principales actividades del tratamiento. El Art.4.16 (*"«establecimiento principal»: […])*, en concreto en el Art.4.16.a y en el Art.4.16.b, indica que normalmente este establecimiento principal tendrá lugar en *"[…] el lugar de su administración central en la Unión […]"*.

- Clase `TratadorPrincipal`: clase que engloba a dos de los principales tipos de tratadores: el responsable y el encargado. Como veremos en sus respectivas clases, tanto el responsable del tratamiento como el encargado de éste comparten muchas funciones, y, por ello, se ha considerado crear una clase que es una generalización con todas aquellas cosas en las que coincidan, y será en las subclases `Responsable` y `Encargado` donde se detallarán los aspectos concretos de cada uno. Los atributos y relaciones de esta clase son los siguientes:
  - `tratamientos`: lista de tratamientos asociados al tratador principal, es decir, aquellos en los cuales interviene. Este atributo tiene su origen en la necesidad estructural por parte del tratador principal de tener acceso en el sistema a dichos tratamientos.
  - `representante`: según el Art.4.17, el tratador principal podrá tener a cargo a un representante que actúe en representación de él y por lo tanto acometa sus funciones: *"«representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;"*. Este atributo será de tipo `Representante`, clase que detallaremos más adelante.

- Clase `Responsable`: clase asociada al responsable del tratamiento. Es importante destacar que dicha clase contará con los atributos, relaciones y métodos tanto de la clase `Tratador` como de la clase `TratadorPrincipal`. Su inclusión en el sistema, además de deberse al constante nombramiento del responsable a lo largo de todo el documento, nace a raíz del Art.4.7: *"«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; […]"*. El responsable del tratamiento, como veremos reflejado en los métodos correspondientes presentes en el anexo B, es la figura encargada de manejar, organizar y controlar el tratamiento. Los atributos de esta clase con los siguientes:
  - `intereses`: según el Art.6.1.f, el responsable tendrá unos intereses a la hora de realizar un tratamiento: *"el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero […]"*.
  - `obligaciones`: según el Art.9.2.b, el responsable del tratamiento tendrá una serie de obligaciones propias del cargo que ostenta: *"el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento […]"*.
  - `derechos`: según el Art.9.2.b mencionado en última instancia, el responsable tendrá una serie de derechos.

- `encargado`: en base a la definición mostrada en el Art.4.8, el responsable del tratamiento podrá tener asociado un encargado: *"«encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;"*. Este atributo `encargado` será de tipo `Encargado`, clase que veremos más adelante.
- `corresponsable`: según el Art.26.1, un responsable podrá trabajar juntamente con otros responsables en el mismo tratamiento: *"Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. […]"*.

- Clase `Encargado`: clase que contiene toda la información asociada al encargado del tratamiento. De la misma forma que la clase `Responsable`, ésta también hereda toda la estructura planteada en nuestra clase `TratadorPrincipal`. Como se ha visto en el Art.4.8 se define la entidad encargado: *"«encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;"*. Los atributos y relaciones de la clase son los siguientes:
  - `autorizacionEncargado`: atributo que almacena el tipo de autorización que recibe el encargado por parte del responsable para poder colaborar en el tratamiento con otro encargado (co-encargado). En el Art.28.2 podemos encontrar la referencia a dicha autorización: *"El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable […]"*. Como siempre, almacenaremos los distintos tipos en un enumerado, ver Anexo A.
  - `coencargado`: atributo de tipo `Encargado` que hace referencia al encargado adicional que cooperará con el ya existente. La posible existencia de un coencargado se contempla en el Art.28.2.
  - `contrato`: según el Art.28.3, existirá un contrato que vincule al encargado con el responsable: *"El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable […]"*. Este contrato será definido en la clase `Contrato` que veremos más adelante.

- Clase `Representante`: clase asociada al representante del tratador principal. Como ya hemos explicado en la clase TratadorPrincipal, según lo visto en el Art.4.17, tanto el responsable como el encargado de tratamiento podrán tener un representante a su cargo que acometa todas sus funciones. Este representante tendrá todas las características de un tratador principal al uso, pero siempre actuará en base a la figura que represente.

- Clase `Contrato`: en relación con lo visto en el Art.28.3, ésta será la clase encargada de almacenar toda la información del contrato realizado entre el encargado y el responsable del tratamiento. Los atributos y relaciones de esta clase son los siguientes:
  - `objeto`: según el Art.28.3, el contrato establecerá el objeto del tratamiento: *"El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la*

duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. […]".
    - duracion: según el Art.28.3, el contrato establecerá la duración del tratamiento.
    - finalidadTratamiento: según el Art.28.3, el contrato establecerá la finalidad del tratamiento. Como sabemos, existen diversos fines posibles todos ellos recogidos en el enumerado correspondiente en el anexo A.
    - tipoTratamiento: según el Art.28.3, el contrato establecerá el tipo del tratamiento.
    - tipoDatosPersonales: según el Art.28.3, el contrato establecerá el tipo de datos personales a tratar (cultural, económico, político, etc).
    - responsable: atributo que contiene al responsable del tratamiento que se ha vinculado con el encargado de este.

- Clase EstablecimientoPrincipal: clase asociada al establecimiento principal, es decir, al lugar de trabajo donde el tratador desempeñará las principales actividades del tratamiento en base a lo recogido en el Art.4.16 visto con anterioridad en la clase Tratador. En este caso, la clase solo contará con un atributo:
    - ubicacion: lugar donde esté ubicado el establecimiento principal.

- Clase Destinatario: como hemos visto con anterioridad, los destinatarios son las entidades encargadas de recibir datos personales de forma indirecta por parte de otros tratadores. Esta clase será la encargada de contemplar dicha figura. Como característica principal tendremos un único método, ver Anexo B.

- Clase Tercero: clase asociada a la figura de una tercera entidad participante en el tratamiento. La definición que aporta el GDPR en el Art.4.10 es la siguiente: *"«tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;"*. El atributo adicional que tendrá esta clase es el siguiente:
    - intereses: según el Art.6.f, un tercero tendrá una serie de intereses a la hora de participar en un tratamiento: *"el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, […]"*.

- Clase DPD: clase asociada a la figura del delegado de protección de datos. El DPD será el encargado de controlar y supervisar si se está llevando a cabo de manera correcta el tratamiento de los datos personales de los interesados. Según el Art.37.1, el DPD será elegido por el responsable y el encargado del tratamiento: *"El responsable y el encargado del tratamiento designarán un delegado de protección de datos […]"*. Los atributos específicos del DPD, en base a lo recogido en el Art.13.1.b (*"los datos de contacto del delegado de protección de datos […]"*), donde habla de sus datos de contacto, se ha decidido que sean los siguientes (también contará con los de la clase Tratador):
    - apellidos: apellidos del DPD.
    - direccion: dirección del DPD.

- `teléfono`: teléfono del DPD.

4.2.5 Paquete UnionEuropea

En este paquete se muestran todas las entidades relacionadas con la Unión Europea. En concreto, se describirán todos los organismos involucrados en el reglamento GDPR. En la Figura 9 se muestran las clases que lo componen.

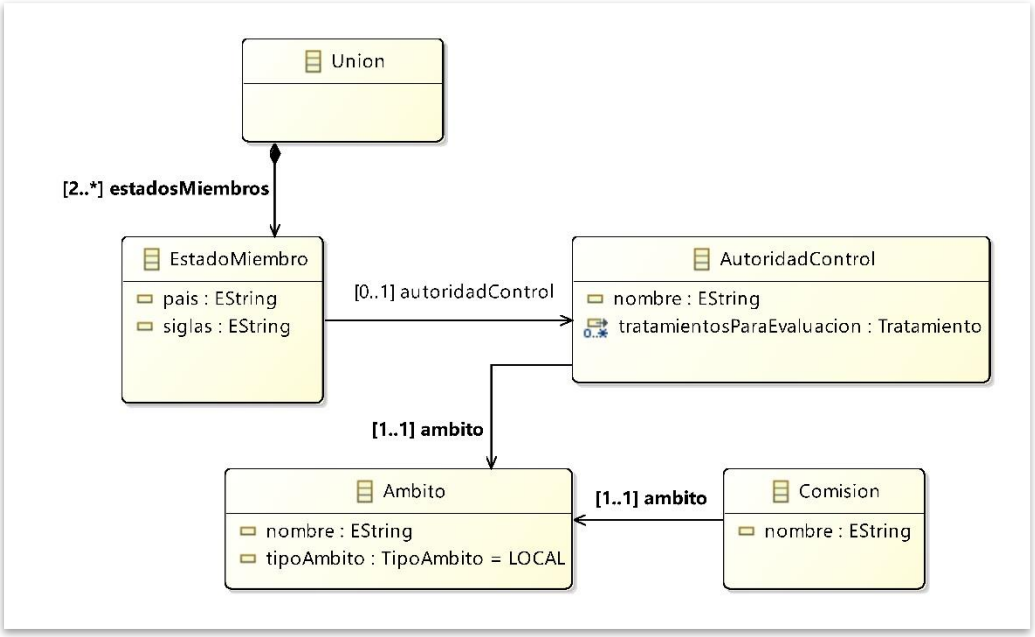

Figura 9: Paquete *UnionEuropea*

- Clase `Union`: clase asociada a la Unión Europea. A lo largo de todo el reglamento GDPR encontramos referencias a la Unión Europea, y es por ello por lo que se ha decidido implementar una clase asociada a dicha entidad. El atributo principal encontrado es el siguiente:
  - `estadosMiembros`: lista con los estados miembros de la Unión Europea. Dentro del reglamento GDPR, en muchas ocasiones se hace referencia a los estados miembros que componen la Unión, por lo que resulta necesario la creación de este tributo para recoger todos y cada uno de ellos. Un ejemplo de ello es el Art.4.16.a: *"en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión […]"*.

- Clase `EstadoMiembro`: clase asociada a un estado miembro. Los atributos de esta clase son los siguientes:
  - `pais`: nombre del estado miembro. Atributo creado con la intención de dotar de un distintivo lógico a cada estado miembro.
  - `siglas`: siglas referentes al nombre del estado miembro. Se ha decidido crear este atributo en base a que cada país, para facilitar la búsqueda dentro del sistema, sería interesante que tuviera una especie de id identificativo, en este caso unas siglas asociadas al nombre.
  - `autoridadControl`: organismo independiente propio de cada estado miembro encargado de velar por la buena realización de los tratamientos. En

el Art.4.21 se define dicha entidad: *"«autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;"*. Más adelante en esta sección realizaremos un análisis más concreto de las posibilidades que aporta la autoridad de control y su estructura.

- Clase `AutoridadControl`: clase que recoge toda la información asociada a las autoridades de control de los estados miembros. Los atributos y relaciones de esta clase son los siguientes:
  - `nombre`: nombre de la autoridad de control. Atributo creado con la intención de dotar de un distintivo lógico a cada autoridad de control.
  - `tratamientosParaEvaluacion`: lista con los tratamientos que requieren una evaluación de impacto (las evaluaciones de impacto fueron comentadas en las secciones 4.2.3 y 4.2.4). Según el Art.35.4, esta lista será creada por la autoridad de control: *"La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos […]"*.
  - `ambito`: ámbito de aplicación en el cual las autoridades de control podrán desarrollar sus funciones. A lo largo de todo el reglamento GDPR, se hacen sucesivas referencias a los ámbitos de aplicación, y, dado que cada autoridad de control tiene su propio rango de acción, se ha decidido implementar un atributo que haga referencia a esto mismo.

- Clase `Ambito`: clase asociada al ámbito de aplicación de una autoridad de control. Los atributos serán los siguientes:
  - `nombre`: nombre del ámbito. Atributo creado con la intención de dotar de un distintivo lógico a cada ámbito.
  - `tipoAmbito`: tipo del ámbito de aplicación en función del área al que aplique: local, regional, nacional o europeo. Este atributo, creado en base a una necesidad lógica, vendrá recogido en un enumerado que como sabemos podremos encontrar en el anexo A.

- Clase `Comision`: clase asociada a la Comisión Europea. Según el Art.45.1, a la hora de transferir datos a un tercer país u organización internacional, será una entidad conocida como Comisión Europea la que evalúe la viabilidad de la transferencia: *"Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado."*. Los atributos y relaciones de esta clase son los siguientes:
  - `nombre`: nombre de la comisión.
  - `ambito`: ámbito de aplicación de la comisión.

4.2.6 Paquete Empresas

En este paquete se muestran todas las entidades relacionadas con las empresas que participan en el tratamiento. Las clases que lo componen son las siguientes, ver Figura 10:

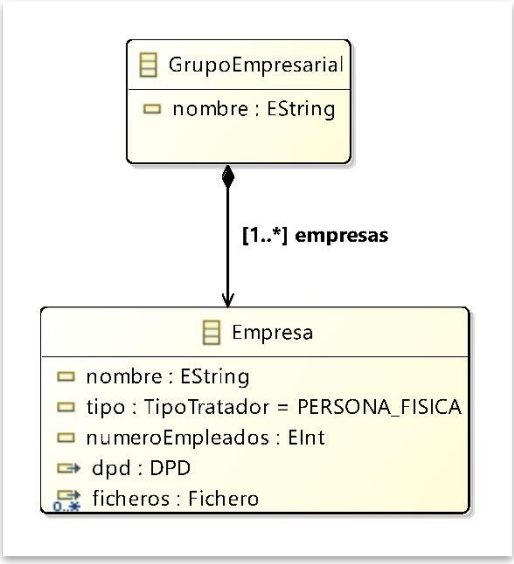

Figura 10: Paquete empresas

- Clase `GrupoEmpresarial`: en base a la definición del Art.4.19 (*"«grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;"*), y al papel que ejerce dicha entidad dentro de los tratamientos, se ha decidido crear una clase asociada a un grupo empresarial. Los atributos y relaciones de esta clase son los siguientes:
  - `nombre`: nombre del grupo empresarial. Atributo creado con la intención de dotar de un distintivo lógico a cada grupo empresarial.
  - `empresas`: lista de las empresas que componen el grupo empresarial en cuestión. A continuación, veremos más en detalle cual es la estructura definida para dichas empresas.

- Clase `Empresa`: clase encargada de almacenar la información de una empresa. Según el Art.4.18, la definición es la siguiente: *"«empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;"*. Los atributos y relaciones de esta clase son:
  - `nombre`: nombre de la empresa. Atributo creado con la intención de dotar de un distintivo lógico a cada empresa.
  - `tipo`: tipo de tratador que representará la empresa. En base a la definición vista en el Art.4.18, la empresa podrá ser asociada con un tipo de tratador de persona física o jurídica.
  - `numeroEmpleados`: número de empleados que tiene la empresa. En el Art.30.5 se hace referencia a dicho número: *"Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas […]"*.
  - `dpd`: según el Art.37.2, una empresa podrá tener un delegado de protección de datos asociado: *"Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento."*.
  - `ficheros`: como es lógico, una empresa tendrá asociados una gran cantidad de ficheros de datos personales.

5 Integración, pruebas y resultados

En esta sección, trataremos de aplicar nuestro modelo obtenido con anterioridad a una situación real y concreta. Se ha tomado como caso de uso un sistema de préstamo de libros en una biblioteca. Una vez hemos elegido, se ha tratado de representar dicho sistema de préstamos en un pequeño diagrama de clases. Para la representación, se ha decidido utilizar la herramienta *Draw.io* [16] debido a su sencillez. La Figura 11 muestra el diagrama de clases de dicha aplicación:

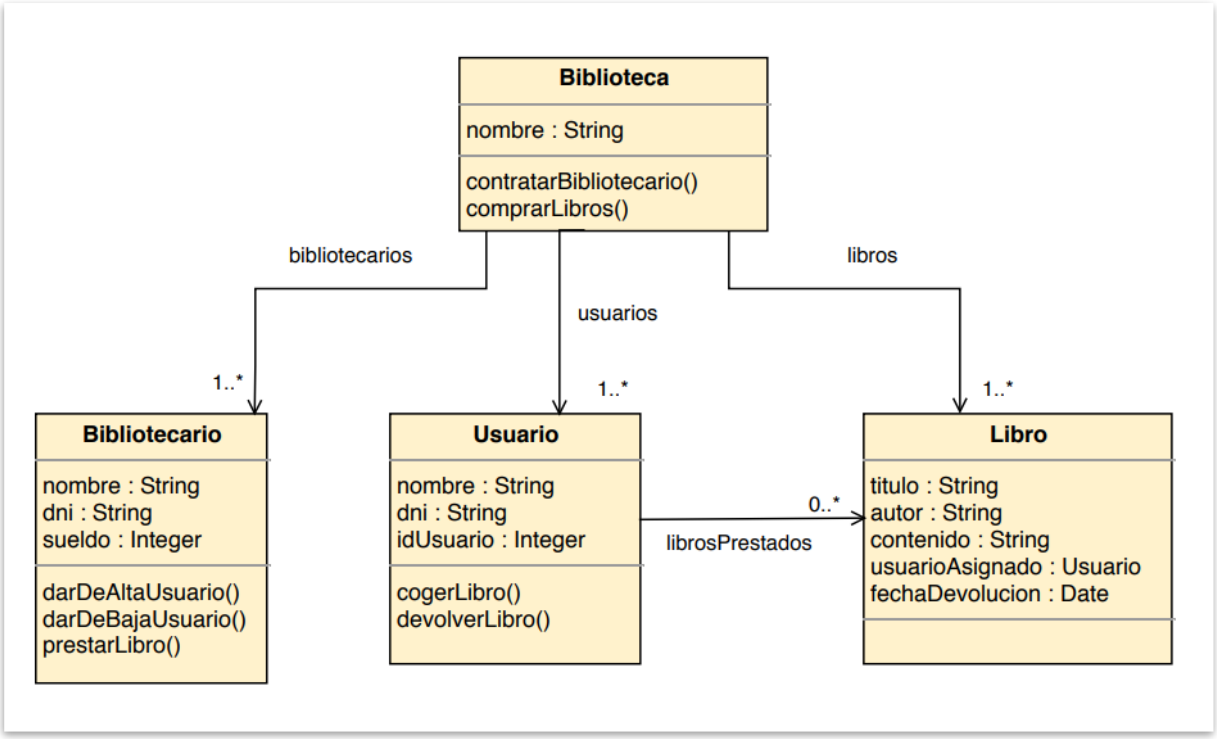

Figura 11: Diagrama de clases de una biblioteca

Como vemos, el diagrama resultante de nuestra biblioteca tiene 4 clases:

- Clase `Biblioteca`: clase representativa de la entidad biblioteca. La biblioteca podrá contratar bibliotecarios y comprar nuevos libros. Además, hay que señalar que tendrá asociadas tres listas de elementos: bibliotecarios, usuarios y libros. En la clase `Biblioteca` se englobarán todos los trabajadores de ésta que no se dediquen al préstamo de libros ni al manejo de los usuarios, funciones asociadas a los bibliotecarios en sí.
- Clase `Bibliotecario`: clase asociada a los empleados principales de una biblioteca. El bibliotecario podrá tanto dar de alta a un nuevo usuario como dar de baja a uno ya existente. Además, será el encargado de prestar los libros a los usuarios.
- Clase `Usuario`: clase encargada de almacenar la información asociada a los usuarios de una biblioteca. La función de los usuarios será la de coger y devolver libros.
- Clase `Libro`: clase que contiene los datos de un libro.

Una vez hemos construido el diagrama base de nuestro ejemplo, procederemos a unificar en un mismo diagrama, y por lo tanto relacionarlos, el modelo del GDPR propuesto en el presente trabajo con el modelo de la biblioteca. Este proceso consistirá en aplicar de manera sencilla y representativa las partes más importantes de nuestro modelo del GDPR a una situación habitual y específica como es el préstamo de libros de una biblioteca. Con ello conseguiremos demostrar la funcionalidad y aplicación real que puede llegar a tener el modelo generado. Se muestra el diagrama resultante en la Figura 12.

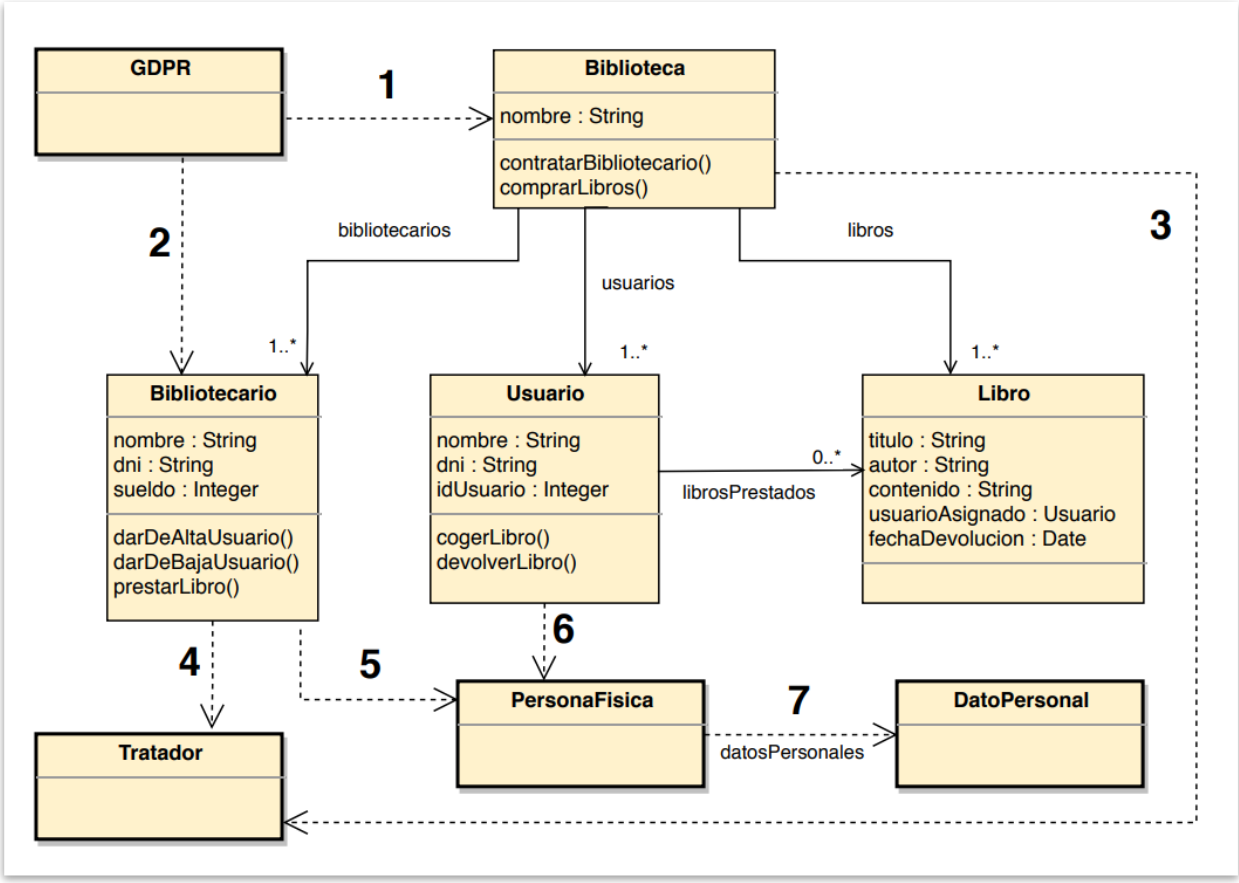

Figura 12: Diagrama de aplicación del modelo GDPR en un sistema bibliotecario

Como vemos, hemos conseguido unificar en un mismo diagrama ambos modelos. Respecto a nuestro modelo del reglamento GDPR, utilizaremos las clases `GDPR`, `Tratador`, `PersonaFisica` y `DatoPersonal` (el resto, con el objetivo de simplificar el diseño, se ha decidido no incluirlo, ya que además alguna de las clases no tenía mucho sentido utilizarlas, como es el caso de las relacionadas con el paquete *Empresas*, ya que se supone que se trata de una biblioteca pública). Como se puede observar, hay dos elementos clave a entender para la explicación del diagrama: las flechas discontinuas, que representan las relaciones entre entidades que explicaremos ahora; y los números en negrita, que nos ayudarán en la explicación a la hora de ubicarnos. A continuación, procedemos a explicar el diagrama en cuestión:

1. El reglamento GDPR, como hemos visto con anterioridad, se basa en desarrollar una forma correcta de actuar en el tratamiento de los datos personales de los interesados por parte de los tratadores. Por ello, en nuestro diagrama, representaremos dicha incidencia del reglamento en las clases o entidades que puedan entenderse como

tratadores dentro del sistema de la biblioteca, ya que estos tendrán que acogerse al mismo. En este primer caso (flecha 1), sabemos que la biblioteca actuará de tratador con respecto a los bibliotecarios y a los usuarios, ya que dispondrá de una base de datos donde almacene y maneje toda la información de estos, por lo que tendrán que acogerse al reglamento para realizar este tratamiento de manera correcta.

2. De la misma manera que el punto (flecha) anterior, el reglamento incidirá sobre los bibliotecarios (y por lo tanto deberán cumplirlo) cuando estos actúen de tratadores en el sistema de altas y bajas de usuarios en la biblioteca.

3. Como hemos hablado, la biblioteca actuará de tratador en la gestión de bibliotecarios y de usuarios, por lo que representaremos una relación entre esta clase y nuestra clase `Tratador`. De esa forma, todo lo contemplado en el paquete *Tratadores* tendrá que ejercerse aplicado a este ejemplo concreto.

4. En este caso, de la misma forma que la clase `Biblioteca`, los bibliotecarios también actuarán de tratadores cuando manejen el sistema de altas y bajas de usuarios y el préstamo de libros. Por ello, representaremos dicho proceso en una nueva relación conectada a la clase `Tratador`.

5. Los bibliotecarios, cuando sus datos sean tratados por la biblioteca, pasarán a formar parte del grupo de interesados. Por este motivo, existirá una relación entre la clase `Bibliotecario` y la clase `PersonaFisica`.

6. De la misma forma que el punto anterior, la relación número 6 se producirá cuando los datos personales de un usuario formen parte de un tratamiento, y por ello, los usuarios de la biblioteca sean considerados como interesados (personas físicas).

7. Por último, y como hemos visto en el análisis del reglamento GDPR, todo interesado tendrá asociados unos datos personales, y es por tanto aquí donde entra en juego nuestra clase `DatoPersonal`.

Resulta importante volver a señalar que todo este proceso es una aplicación simplificada y esquemática de las principales clases del reglamento. No obstante, en base a lo visto con anterioridad, podemos concluir que nuestro modelo del reglamento GDPR puede aplicarse directamente en situaciones reales y específicas. De igual manera, podríamos aplicarlo a otro tipo de contextos, como, por ejemplo, el sistema de usuarios de un gimnasio o la aplicación móvil de citas de una clínica dental. Si en un futuro se decidiese aplicarlo de forma completa y detallada, una buena manera de comprobar si se ha acoplado al sistema con éxito sería por ejemplo rellenar el formulario [17] que la Agencia Española de Protección de Datos pone a disposición de los DPD para que comprueben el cumplimiento del reglamento GDPR.

6 Conclusiones y trabajo futuro

6.1 Conclusiones

El objetivo de este TFG, como comentamos al comienzo, se basa en analizar y realizar una representación en forma de modelo del reglamento GDPR, de tal forma que sea posible no solo una interpretación más sencilla del mismo, sino también que consigamos obtener una estructura aplicable a situaciones específicas en las cuales exista tratamiento de datos personales, con el fin de comprobar y controlar el cumplimiento del reglamento. Además, como hemos comentado con anterioridad, buscamos cambiar el momento de aplicación de los requisitos legales, es decir, se pretende disponer de ellos ya en fase de diseño, de tal forma que el desarrollo del proyecto o aplicación en cuestión se realice en base al reglamento GDPR garantizando su cumplimiento desde un primer momento.

Tras haber desarrollado el modelo, y haber cumplimentado las pruebas correspondientes, podemos afirmar que hemos sido capaces de interpretar y analizar todas y cada una de las disposiciones que recoge el extenso reglamento GDPR (99 artículos en total). Dicho proceso, debido a la extensión de la norma, y al análisis manual de los artículos, ha resultado extenso y laborioso, pero, una vez finalizado, podemos concluir que gracias a él se ha conseguido adquirir una noción verdaderamente grande de lo que dicta el reglamento GDPR y sus objetivos, así como conocimiento en profundidad del campo de la protección de datos de carácter personal. En lo que respecta al propio reglamento GDPR, hemos visto como esta nueva legislación protege de manera mucho más eficaz a los interesados, ya que se lleva un control mucho más exhaustivo de los tratamientos, y por ello de los datos personales. Por este motivo, los tratadores tienen que realizar ahora esfuerzos mucho más intensos para asegurarse del cumplimiento de todos y cada uno de los artículos, pero se espera que, con trabajos como este, donde se proceda a modelar y estructurar el reglamento, todos consigan cumplir con lo establecido y asegurarse de esa forma de realizar un tratamiento completamente seguro y eficaz.

En cuanto a la aplicación de nuestro modelo a una situación específica (ver Sección 5), podemos decir que hemos comprobado cómo podemos llevar nuestro modelo a cualquier tipo de lugar o situación donde se estén tratando los datos personales de los interesados, y aplicarlo de manera eficaz y precisa. Además, en base a esto último, podemos afirmar que somos capaces de realizar dicho proceso de aplicación al comienzo del ciclo de vida de un producto, ya que bastará con utilizar el modelo creado junto con el relativo al proyecto que se esté analizando, tras lo cual dispondremos de la implementación de los requisitos legales asociados al reglamento GDPR, y podremos por lo tanto trabajar con ellos desde el comienzo del proyecto, más concretamente en la fase de diseño, y realizar el desarrollo en base a los mismos.

6.2 Trabajo futuro

En lo que respecta al posible trabajo futuro, tendremos varias opciones. Una de ellas, consistirá en analizar todas las restricciones que tiene el reglamento. Con restricción nos referimos por ejemplo a ese tipo de artículos en los que se indica cierto procedimiento, pero se aclara que solo será posible cuando se den ciertas condiciones. Analizar dichas condiciones, y, relacionarlas con los atributos obtenidos, podría ser una buena manera de

que nuestro modelo ganase en portabilidad a la par que fuese más específico, todo ello sin perder su capacidad para ser aplicado en todos los contextos.

Por otro lado, en un futuro, nos podríamos centrar en aumentar el ámbito de aplicación de nuestro modelo. Para ello, sería un buen punto de inicio fijarse no solo en los artículos relacionados con el tratamiento de los datos como tal, sino también en los artículos donde se recoge como debe ser el comportamiento entre organizaciones y la comunicación entre ellas.

En cuanto a la validación final del modelo, podría realizarse una aplicación formal y completa del mismo en un sistema específico y real más extenso que el comentado en la sección 5, donde viésemos con más detalle si nuestro modelo es capaz, en todas sus variantes, de conseguir lo que se propone, es decir, comprobar que es válido y aplicable para cualquier tipo de contexto por complejo que este sea.

Por último, tras haber realizado un análisis y modelado del reglamento GDPR, que aplica a nivel europeo, podría utilizarse el producto obtenido para que, tras realizar un análisis, se modelase la "*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales"* [3], la cual aplica a nivel territorial español. Este nuevo desarrollo consistiría en desarrollar un modelo específico del reglamento GDPR en base a la ley española anteriormente mencionada.

Referencias

[1] Parlamento Europeo y Consejo Europeo, *Reglamento General de Protección de Datos,* 2016.

[2] Parlamento Europeo y Consejo Europeo, *Directiva 95/46/CE,* 1995.

[3] Estado Español, *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales,* 2018.

[4] D. Torre, G. Soltana, M. Sabetzadeh, L. C. Briand, Y. Auffinger y P. Goes, «Using Models to Enable Compliance Checking against the GDPR: An Experience Report,» *22nd {ACM/IEEE} International Conference on Model Driven Engineering Languages and Systems, {MODELS} 2019, Munich, Germany, September 15-20, 2019,* pp. 1-11, 2019.

[5] A. Rabinia, S. Ghanavati, L. Humphreys y T. Hahmann, «A Methodology for the Formal Legal_GRL Framework: A Research Preview,» *Requirements Engineering: Foundation for Software Quality - 26th International Working Conference, {REFSQ} 2020, Pisa, Italy, March 24-27, 2020, Proceedings {[REFSQ} 2020 was postponed]*, vol. 12045, pp. 124-131, 2020.

[6] G. Blanco-Lainé, J.-S. Sottet y S. Dupuy-Chessa, «Using an enterprise architecture model for GDPR compliance principles,» *The Practice of Enterprise Modeling - 12th {IFIP} Working Conference, PoEM 2019, Luxembourg, Luxembourg, November 27-29, 2019, Proceedings,* vol. 369, pp. 199-214, 2019.

[7] P. Beauvoir y J.-B. Sarrodie, «archimatetool,» [En línea]. Available: https://www.archimatetool.com/.

[8] C. E. Montenegro, J. M. Cueva, Ó. Sanjuán y P. A. Gaona, «Desarrollo de un lenguaje de dominio específico para sistemas de gestión de aprendizaje y su herramienta de implementación "KiwiDSM" mediante ingeniería dirigida por modelos,» *Ingeniería,* vol. 15, nº 2, pp. 67-81, 2010.

[9] O. M. Group, «uml.org,» [En línea]. Available: https://www.uml.org/.

[10] D. C. Schmidt, «Guest Editor's Introduction: Model-Driven Engineering,» *{IEEE} Computer,* pp. 25-31, 2006.

[11] E. Foundation, «eclipse,» [En línea]. Available: https://www.eclipse.org/ide/.

[12] V. P. I. Ltd., «visual-paradigm.com,» [En línea]. Available: https://www.visual-paradigm.com/.

[13] S. Systems, «sparxsystems.com,» [En línea]. Available: https://sparxsystems.com/.

[14] E. Foundation, «eclipse,» [En línea]. Available: https://www.eclipse.org/modeling/emf/.

[15] A. S. S. D. GmbH, «atlasti.com,» [En línea]. Available: https://atlasti.com/.

[16] Atlassian, «draw.io,» [En línea]. Available: https://www.draw.io/.

[17] A. E. d. P. d. Datos, *Listado de cumplimiento normativo,* 2018.

[18] «definicion.de,» [En línea]. Available: https://definicion.de/plugin/.

Glosario

GDPR	General Data Protection Regulation
MDE	Model-driven engineering
EMF	Eclipse Modeling Framework
TFG	Trabajo fin de Grado
FLG	Formal Legal_GRL Framework
EAM	Modelos de la arquitectura de la empresa
DPD	Delegado de protección de datos
UML	Unified Modeling Language
DSL	Domain Specific Language

Anexos

A Paquete Enumerados

En este anexo, procedemos a mostrar el paquete *Enumerados* de nuestro modelo, obtenido a partir del análisis del reglamento GDPR. Como se ha mencionado con anterioridad en la sección 4.2, este paquete será el formado por la información relacionada con todos aquellos atributos del modelo que constituyesen una enumeración de distintos tipos de cualidades concretas. Los enumerados obtenidos son los que podemos ver en la siguiente figura:

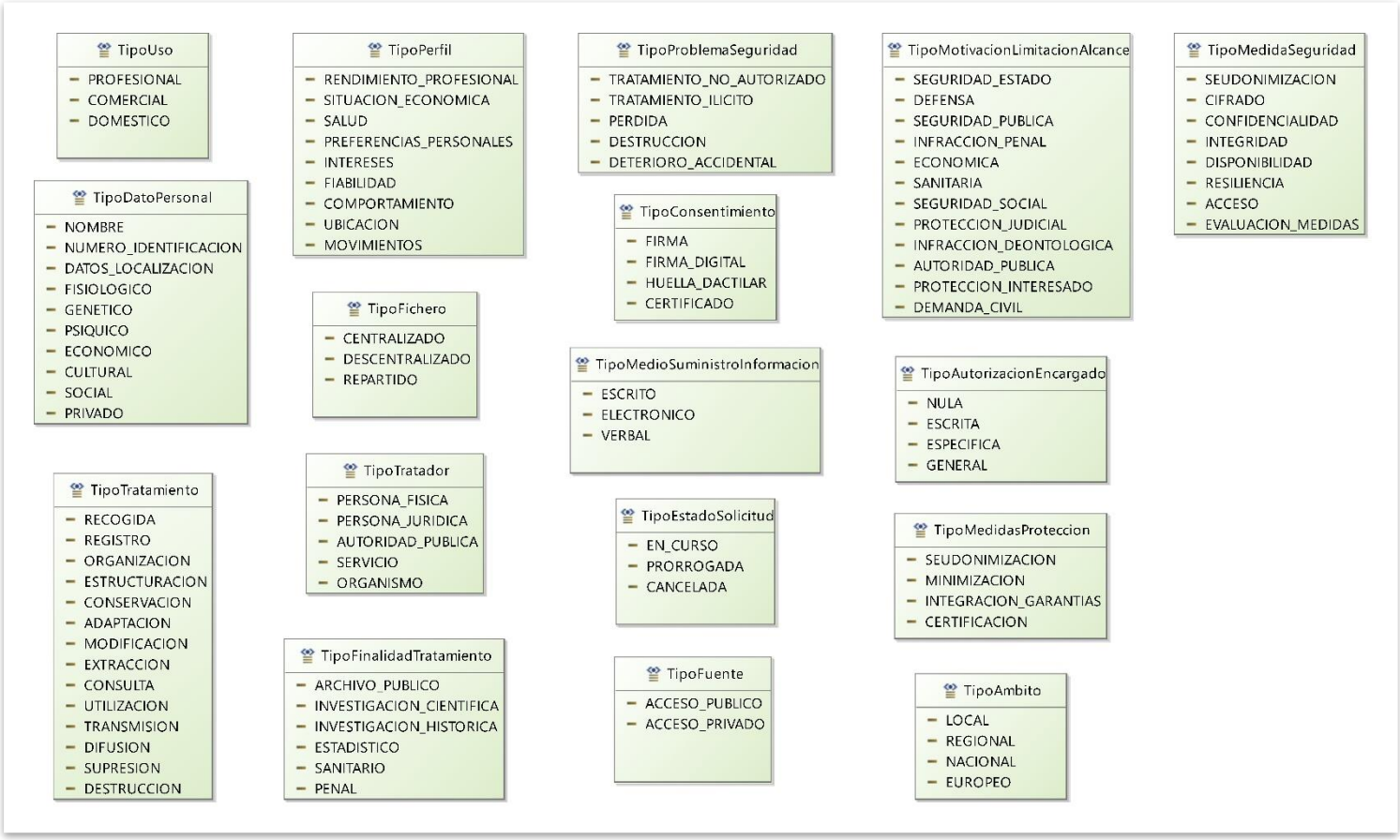

Figura 13: Paquete *Enumerados*

B Diagramas completos y explicación de métodos

En esta sección, procederemos a explicar los métodos de los paquetes, así como a mostrar los diagramas completos obtenidos durante el desarrollo del modelo del reglamento GDPR. Hay que destacar que solo mostraremos aquellos paquetes que tengan métodos (y dentro de los paquetes solo las clases afectadas), razón por la cual están incompletos en la sección 4.2, es decir, no mostraremos de nuevo ni el paquete *Ley* ni el de *Empresas*, ya que carecen de métodos (ni detallaremos de nuevo las clases que no tengan métodos).

- Paquete *Interesados*

  - Métodos de la clase `PersonaFisica`:

    - `darConsentimiento()`: el interesado, según el Art.4.11, podrá proporcionar su consentimiento para que sus datos personales sean tratados: *"«consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;"*.
    - `retirarConsentimiento()`: según el Art.7.3 *("El interesado tendrá derecho a retirar su consentimiento en cualquier momento. […]"*), toda persona física podrá si así lo desea retirar el consentimiento que previamente dio para el tratamiento de sus datos personales.
    - `modificarDatosPersonales()`: según el Art.16, conocido como *"Derecho de rectificación"*, el interesado podrá modificar sus datos personales si así lo desea *("El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos […]"*).
    - `presentarReclamacion()`: en el Art.13.2.d se nombra la posibilidad que tendrá el interesado de presentar una reclamación de no estar conforme con alguna parte del tratamiento: *"el derecho a presentar una reclamación ante una autoridad de control;"*.
    - `transmitirDatosTratamiento()`: como indica el Art.20.1, *"El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento […]"*.

  A continuación, mostramos el diagrama completo del paquete:

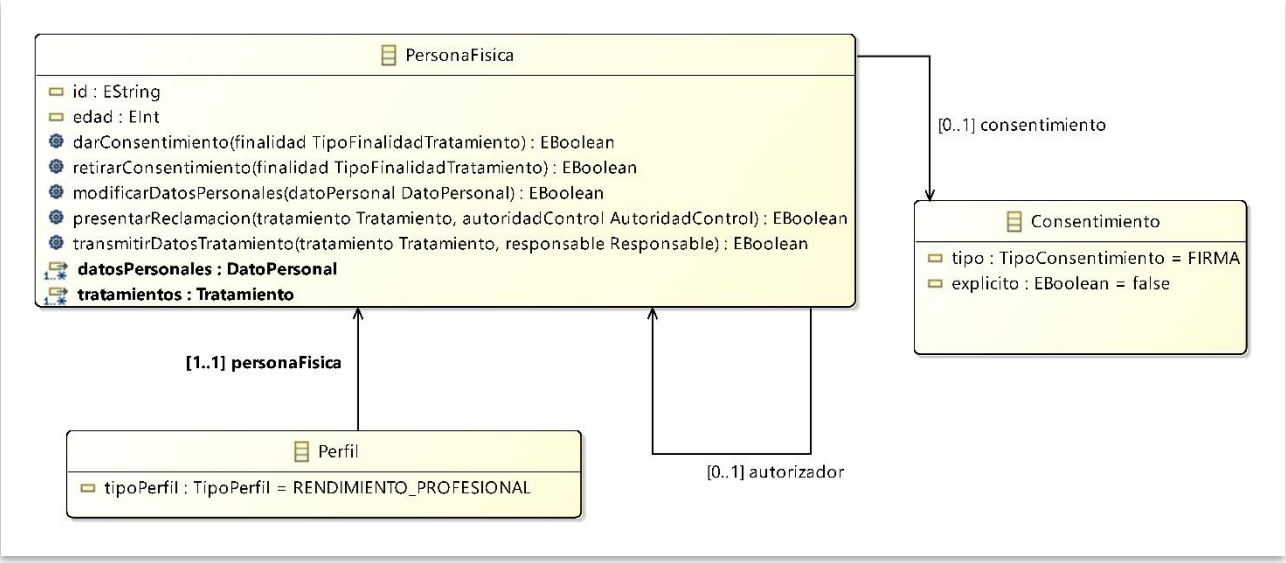

Figura 14: Paquete *Interesados* completo

- Paquete *DatosPersonales*

  - Métodos de la clase `Tratamiento`:

    - `solicitarInformacionTratamiento()`: el interesado, según el Art.15.1, podrá solicitar parte de la información correspondiente al tratamiento de sus datos personales: *"El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información: […]"*. En los subapartados del Art.15.1 se detalla esta información. Como se observa en la sección 4.2.3, en la clase `SolicitudInformacionTratamiento` se detalla la estructura que recibirá el interesado tras la solicitud mencionada.
    - `solicitarRectificacionTratamiento()`: según el Art.15.1.e, el interesado podrá solicitar la rectificación de los datos personales asociados al tratamiento: *"[…] solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales […]"*.
    - `solicitarSupresionTratamiento()`: como hemos visto con anterioridad en el Art.15.1.e, el interesado podrá solicitar la supresión de los datos personales asociados al tratamiento.
    - `solicitarLimitacionTratamiento()`: en base a lo visto en el Art.15.1.e, el interesado podrá solicitar la limitación del tratamiento.
    - `solicitarListaDestinatarios()`: de la misma forma que los casos anteriores y, como hemos observado en el Art.13.1.e, los interesados podrán solicitar la lista de los destinatarios del tratamiento de sus datos: *"los destinatarios o las categorías de destinatarios de los datos personales, en su caso;"*.

A continuación, mostramos el diagrama completo del paquete:

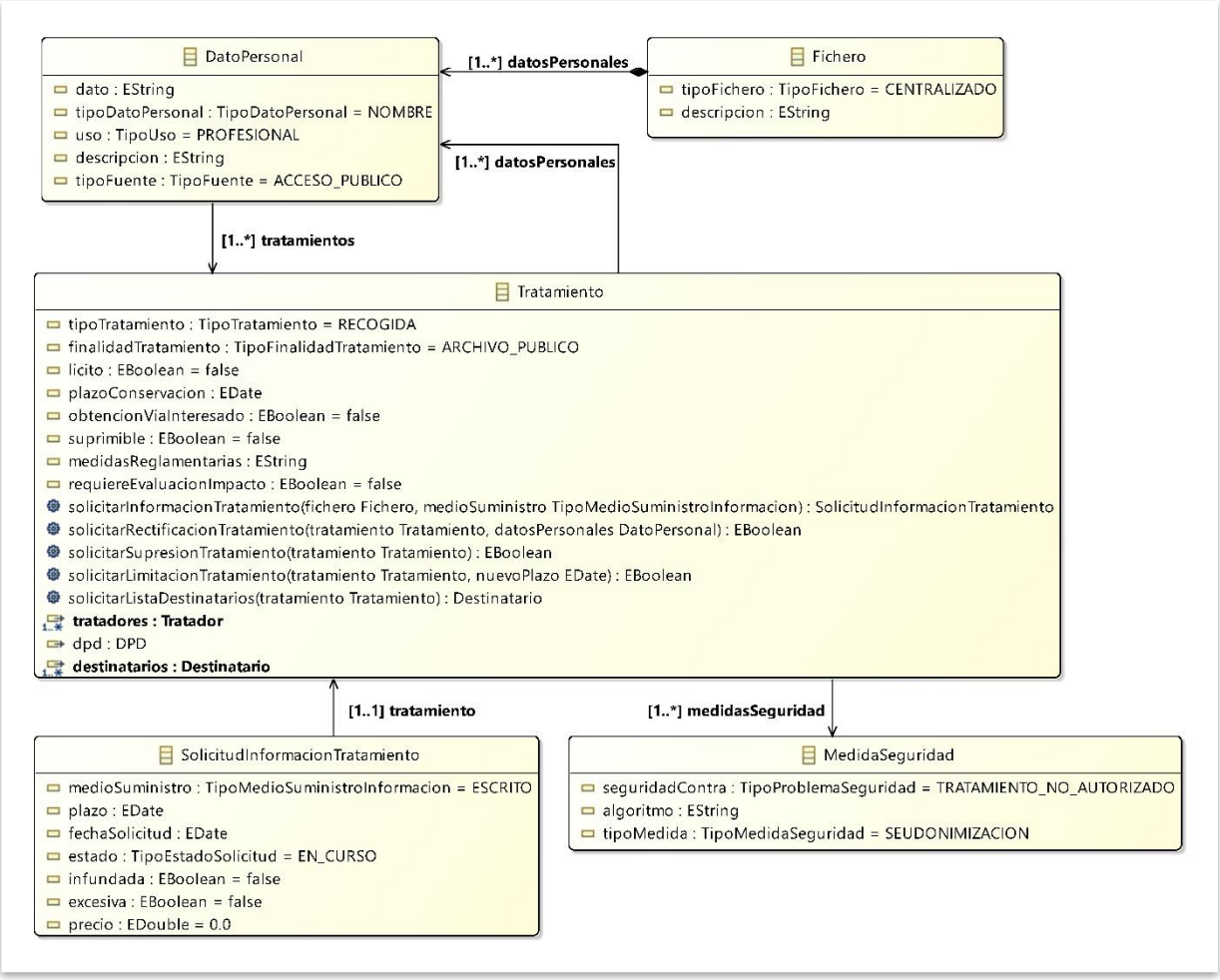

Figura 15: Paquete *DatosPersonales* completo

- Paquete *Tratadores*

  - Métodos de la clase `Tratador`:

    - `ejercerArticulo()`: método representativo que hace referencia a la capacidad del tratador de ejercer un artículo del reglamento GDPR en lo que respecta al tratamiento de los datos.
    - `verificarConsentimiento()`: el tratador deberá comprobar que el interesado ha dado su consentimiento para el tratamiento de sus datos personales. En el Art.7.1, en el caso del responsable, se informa de ello: *"Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales."*.

  - Métodos de la clase `TratadorPrincipal`:

    - `designarRepresentante()`: según el Art.4.17, el tratador principal podrá designar un representante que actúe en representación de él y por lo tanto acometa sus funciones: *"«representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;"*.
    - `aplicarMedidasReglamentarias()`: como vimos en la sección 4.2.3, en la clase `Tratamiento`, los tratamientos tendrán una serie de medidas aplicadas que garanticen el cumplimiento del reglamento GDPR. Dichas medidas serán aplicadas por el tratador principal. Si nos fijamos por ejemplo en la figura del responsable del tratamiento, según el Art.24.1 tenemos que: *"[...] el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento [...]"*.
    - `notificarViolacion()`: el tratador principal deberá notificar las violaciones de seguridad que puedan surgir en el tratamiento de los datos personales del interesado. Según el Art.33.1, el responsable deberá hacerlo a la autoridad de control (elemento que veremos en la sección 4.2.5): *"En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control [...]"*. En el caso del encargado, según el Art.33.2, dicha comunicación se hará al responsable del tratamiento: *"El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento."*.
    - `evaluacionImpactoTratamiento()`: como vimos en la sección 4.2.3, en la clase `Tratamiento`, cuando los tratamientos entrañen peligro para los derechos y libertades del interesado, estos requerirán una evaluación exhaustiva del impacto que pueda ocasionar. En el Art.35.1, en el caso del responsable, vemos la referencia a dicho procedimiento: *"[...] el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales [...]"*.

- `consultarAutoridadControl()`: si tras realizar una evaluación de impacto, el tratador principal observa que el tratamiento entraña mucho peligro, este deberá consultar a la autoridad de control para que determine si ha de realizarse dicho tratamiento. Todo ello queda reflejado en el Art.36.1: *"El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo […]"*.
- `designarDPD()`: el tratador principal, si las circunstancias lo permiten, podrá designar un delegado de protección de datos en base a lo recogido en el Art.37.1: *"El responsable y el encargado del tratamiento designarán un delegado de protección de datos […]"*.
- `transferirDatosPersonales()`: en ocasiones el tratador principal transmitirá los datos personales del interesado a un destinatario. Si nos fijamos por ejemplo en el responsable, en el Art.14.f tendremos lo siguiente: *"[…] la intención del responsable de transferir datos personales a un destinatario […]"*.

– Métodos de la clase `Responsable`:

- `determinarFinalidadTratamiento()`: como indica el Art.4.7, el responsable del tratamiento determinará la finalidad de este: *"«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; […]"*.
- `determinarMediosTratamiento()`: de nuevo, en base a lo visto en el Art.4.7, sabemos que el responsable tendrá la capacidad de determinar los medios del tratamiento.
- `facilitarInformacionTratamiento()`: como ya hemos comentado con anterioridad en la clase `Tratamiento`, el responsable transmitirá la información del tratamiento al interesado cuando este la requiera vía solicitud.
- `prorrogarPlazoSolicitud()`: según lo visto en el art.12.3, el responsable tendrá la capacidad de establecer una prórroga de la solicitud de la información del tratamiento enviada por el interesado: *"[…] Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas […]"*.
- `comunicarCancelacionSolicitud()`: el responsable podrá cancelar una solicitud de información del tratamiento de un interesado, así lo indica el Art.12.5.b: *"negarse a actuar respecto de la solicitud."*. Destacar que esto será así bajo unas condiciones específicas en las cuales la solicitud del interesado sea calificada como infundada o excesiva. Una vez cancelada, el responsable se lo comunicará al interesado.
- `solicitarInformacionInteresado()`: en base a lo que indica el Art.12.6, el responsable podrá solicitar cierta información extra al interesado: *"[…] cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se*

refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.".

- `comunicarModificacionTratamiento()`: según el Art.19, el responsable del tratamiento comunicará a los destinatarios cualquier tipo de modificación que haya sufrido el tratamiento o los datos personales asociados a él: *"El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales […]"*.
- `transmitirInformacionTratamiento()`: según el Art.20.2: *"[…] el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable. […]"*.
- `designarEncargado()`: el responsable elegirá un encargado. Esto queda recogido en el Art.28.1: *"Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado […]"*.
- `comunicarViolacion()`: el responsable comunicará al interesado, si es necesario, la violación de sus derechos y libertades. En el Art.34.1 se indica lo siguiente con respecto a lo anterior: *"Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida."*.

– Métodos de la clase `Encargado`:

- `tratamientoDatos()`: en base a la definición de encargado reflejada en el Art.4.8, el encargado tendrá como cometido principal tratar los datos personales: *"«encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;"*.
- `actualizarDatos()`: método que permite al encargado actualizar los datos personales de la persona física. Tiene su origen en la necesidad estructural de acotar dicha funcionalidad.
- `borrarDatos()`: método que permite al encargado borrar los datos personales de la persona física. Tiene su origen en la necesidad estructural de acotar dicha funcionalidad.

– Métodos de la clase `Destinatario`:

- `recibirDatos()`: como sabemos, el responsable del tratamiento transmitirá los datos relacionados con el tratamiento a los destinatarios asociados, así como las modificaciones recogidas en el Art.19: *"El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales […]"*. Por ello, se ha decidido implementar este método como función representativa del destinatario.

– Métodos de la clase `Tercero`:

  - `tratamientoDatos()`: como entidad adicional del tratamiento, y considerándose un tratador, el tercero tendrá la capacidad de tratar los datos.
  - `actualizarDatos()`: método que permite a un tercero actualizar los datos personales de la persona física. Tiene su origen en la necesidad estructural de acotar dicha funcionalidad.
  - `borrarDatos()`: método que permite a un tercero borrar los datos personales de la persona física. Tiene su origen en la necesidad estructural de acotar dicha funcionalidad.

– Métodos de la clase `DPD`:

  - `supervisarProteccionDatos()`: el DPD, debido a las funciones diversas recogidas en el Art.39, tendrá en este método una función que aglutine de alguna manera todas ellas y sea representativo de la capacidad de acción que tendrá dentro del tratamiento. Este método, en base a la función principal del DPD representada en el Art.39.1.b (*"supervisar el cumplimiento de lo dispuesto en el presente Reglamento […]"*), será denominado como `supervisarProteccionDatos()`.

A continuación, en la siguiente página mostramos el diagrama completo del paquete:

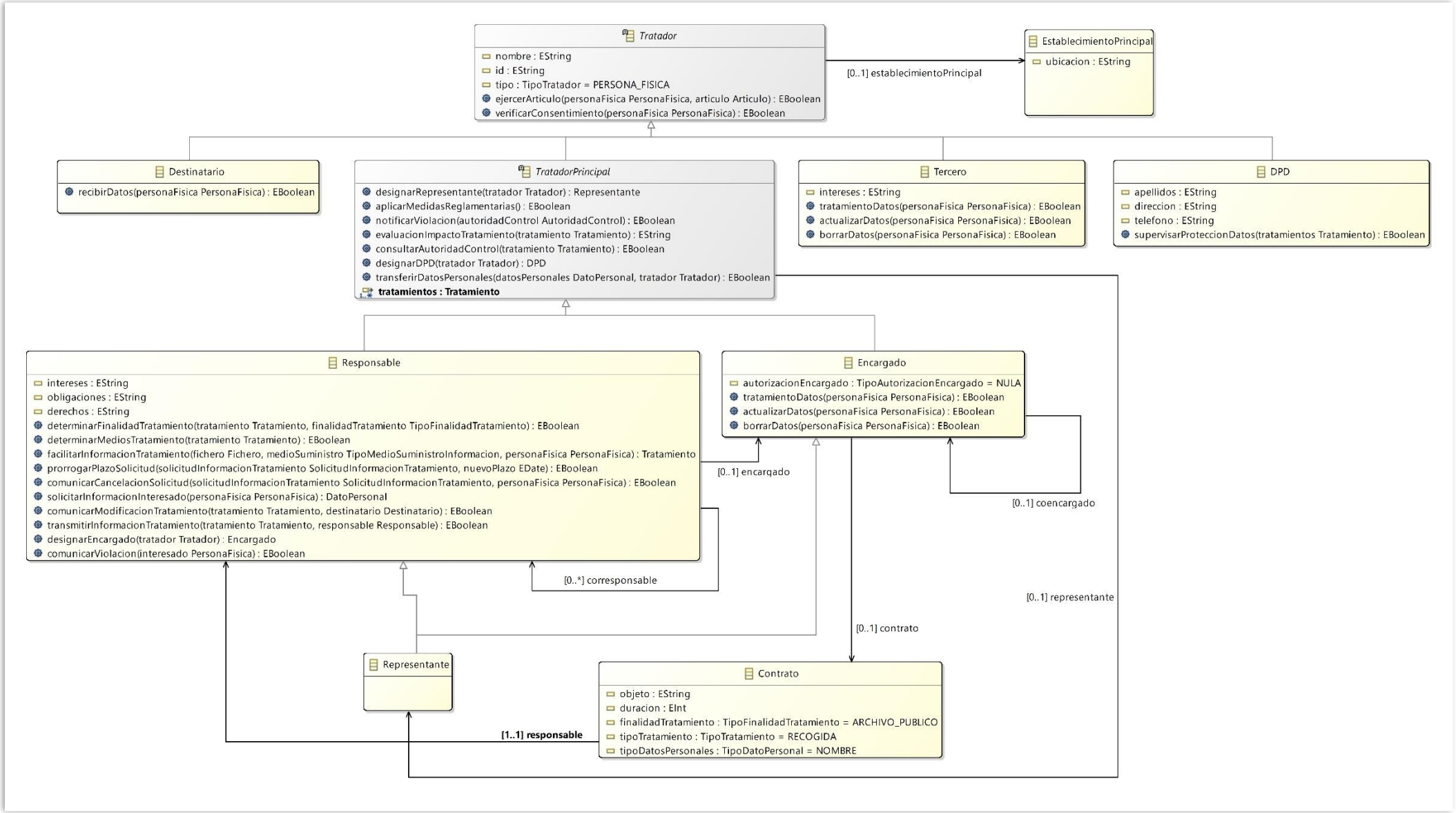

Figura 16: Paquete *Tratadores* completo

- Paquete *UnionEuropea*

  - Métodos de la clase `Union`:

    - `limitarAlcance()`: la Unión Europea podrá limitar el alcance del tratamiento según el Art.23.1: *"El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34 […]"*.

  - Métodos de la clase `EstadoMiembro`:

    - `establecerAutoridadControl()`: según el Art.4.21, cada estado miembro será el encargado de establecer su autoridad de control: *"«autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;"*.
    - `introducirDisposicion()`: según el Art.6.2, los estados miembros podrán añadir disposiciones: *"Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento […]"*.
    - `introducirCondicion()`: en ciertas circunstancias, según el Art.9.4 los estados miembros tendrán la potestad y capacidad de añadir condiciones al tratamiento: *"Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."*.

  - Métodos de la clase `AutoridadControl`:

    - `requierenEvaluacionImpacto()`: la autoridad de control, en base a lo recogido en el Art.35.3, analizará cuales son los tratamientos que requieren una evaluación de impacto: *"La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos […]"*.
    - `tratarReclamacion()`: según el Art.4.22.c, los interesados presentarán reclamaciones a la autoridad de control pertinente: *"se ha presentado una reclamación ante esa autoridad de control;"*.
    - `limitarTratamiento()`: según el Art.58.f, la autoridad de control podrá: *"imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;"*.
    - `autorizarTratamiento()`: según lo visto en el Art.36.1, cuando el responsable haya realizado una evaluación de impacto y no esté seguro de la seguridad del tratamiento este deberá consultar a la autoridad de control, tras lo cual será esta la que tendrá la potestad de autorizar o no el tratamiento: *"El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo […]"*.

– Métodos de la clase `Comision`:

  - `evaluarTransferenciaDatos()`: según el Art.45.1, a la hora de transferir datos a un tercer país u organización internacional, será la Comisión Europea la que evalúe la viabilidad de la transferencia: *"Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado."*.

A continuación, mostramos el diagrama completo del paquete:

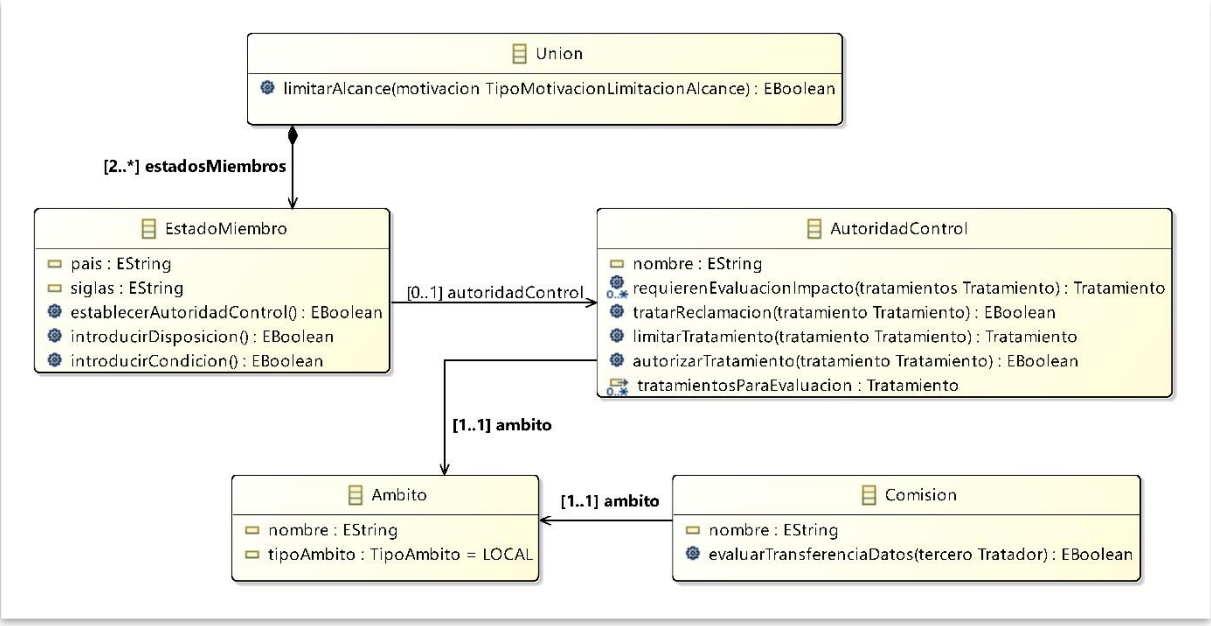

Figura 17: Paquete *UnionEuropea* completo