Deusto
Facultad de Ingeniería
Ingeniaritza Fakultatea

Grado en Ingeniería Informática

Informatikako Ingeniaritzako gradua

Proyecto fin de grado

Gradu amaierako proiektua

Estudio sobre la privacidad en el aprendizaje federado mediante el desarrollo de un sistema de recomendación online

Ibai Guilén Pacho

Director: Diego Casado Mansilla

Bilbao, mayo de 2021

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

En esta memoria se detalla el estudio sobre la tecnología del Federated Learning, aprendizaje federado, y su implementación en un sistema de recomendación. Esta tecnología es diferente al clásico aprendizaje automático, el cual reune toda la información en un único dispositivo que se encarga de realizar las operaciones de computación y de creación de los modelos de inteligencia artificial. Gracias al aprendizaje federado se consigue que se puedan crear diferentes modelos de inteligencia artificial distribuidos en los participantes de la red de aprendizaje, de forma que cada participante conserve su información en su dispositivo y que gracias a un mecanismo de agregación global se consiguen agregar los modelos de los diferentes participantes para mejorar el modelo de cada uno de ellos redistribuyendolo.

En los diferentes apartados se podrá encontrar la siguiente información sobre el proyecto:

- **Antecedentes y justificación**, en esta sección se detallan los acontecimiento y motivaciones que han promovido el desarrollo de este proyecto.
- **Obejtivos y alcance**, apartado en el que se especifican los objetivos que se persiguen en el proyecto tanto en cuanto a la investigación como en cuanto al desarrollo.
- **Metodología**, hoja de ruta y forma de trabajar que se ha cumplido durante todo el proyecto.
- **Planificación**, listado de tareas y planificación a lo largo del cuatrimestre para la correcta gestión de tiempos en este proyecto.
- **Introducción al Federated Learning**, breve descripción de lo que consiste la tecnología, fundamentos y problemas.

- **Desarrollo**, apartado principal del proyecto, en este se puede encontrar tanto información sobre los requisitos, la gestión de riesgos, la arquitectura del sistema, el sistema de agregación desarrollado, resultados de los experimentos, ...
- **Presupuesto**, listado de materiales, precio y horas dedicadas al proyecto.
- **Anexo**, información relativa a la protección de datos en la Unión Europea y España.

1.1. Consideraciones éticas

En este proyecto surgen dos grandes consideraciones éticas, la de la legalidad y la de la defensa del derecho a la privacidad en la era digital.

1.1.1. Legalidad

Según el principio de legalidad del código ético y deontológico de la Ingeniería Informática [1], artículo 7, punto 5, el sistema ha de cumplir tanto con las legislaciones Españolas como Europeas.
La solución propuesta al problema de agregación de distintas inteligencias artificiales viene de la privacidad como patrón de diseño, motivo y objetivo principal del proyecto. Con este sistema se pretende cumplir tanto con la legislación vigente como con la pionera carta de derechos digitales de España (Anexo**??**, Derechos fundamentales**??**) que entrará en vigor en los próximos años.
En esta carta existen dos puntos de gran impacto para este proyecto: los derechos ante la Inteligencia Artificial (Derecho XXIII) y el derecho a no ser localizado y perfilado (Derecho V). Ambos explicados en el apartado de derechos fundamentales del Anexo.
Respondiendo a los derechos en cuanto al perfilado de usuarios, es la propia tecnología (federated learning) la que obliga a su consentimiento, ya que la tecnología parte de la premisa de que los usuarios que participan en la red participan de mutuo acuerdo. Es decir, ningún tipo de red que implemente el federated learning podrá incumplir esta ley puesto que para entrar en la red hace falta expresarlo explícitamente.
Sobre los derechos ante la inteligencia artificial el usuario tendrá derecho en todo momento a impugnar la recomendación e incluso a corregirla si así lo desea.
Para cumplir con la RGPD(Explicado en el apartado de legislación del Anexo) el propio dispositivo del usuario tiene en su poder el modificar sus datos en caso de que sean inexactos o eliminarlos si desea borrar su huella digital. Por lo cual siempre estará en su mano y bajo su responsabilidad el cómo se utilizan sus datos.

1.1.2. Derechos a la privacidad

Cabe destacar como un pequeño apunte que el tema de la privacidad digital es muy controversial, hay expertos que defienden que la privacidad es la privacidad y no se deben hacer distinciones entre lo digital y lo no digital, otros sin embargo, hacen referencia a que es necesaria una nueva generación de los derechos humanos.

En artículos como el "Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica" [2] del Dr. Javier Bustamante Donas ya se hacía referencia al camino hacia la cuarta generación de los derechos humanos por la tecnologización de la sociedad. En este artículo, el Dr. Javier Bustamante expone varios ejemplos para demostrar la importancia de los derechos digitales. Uno de estos ejemplos es que si se restringe el libre acceso y libre uso de la tecnología se está atentando directamente contra a la libertad de opinión y expresión. Otro claro ejemplo que expresa es el de la censura en China, que es de especial relevancia puesto que afecta a un porcentaje significativo de la sociedad. El caso es que china ha implantado barreras informáticas que impiden la consulta y la visualización de cualquier tipo de páginas web no autorizadas por el gobierno. Además, todo ciudadano chino debe completar un formulario exhaustivo antes de acceder a internet, haciéndolo fácilmente identificable en la red.
Sea como fuere, en estos momentos España se encuentra redactando una carta sobre la privacidad digital que tendrá un gran impacto en la sociedad y en internet. Supone un hito en Europa y en el mundo que un estado se comprometa a la protección de los derechos digitales de sus ciudadanos, para más información me remito al apartado Derechos fundamentales del Anexo.

Bibliografía

[1] *Código Ético y Deontológico de la Ingeniería Informática*, es-es, https://ccii.es/CodigoDeontol

[2] D. J. B. Donas, "HACIA LA CUARTA GENERACIÓN DE DERECHOS HUMANOS: REPENSANDO LA CONDICIÓN HUMANA EN LA SOCIEDAD TECNOLÓGICA," es, pág. 24,