



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

1. Antecedentes y justificación	1
1.1. Antecedentes	1
1.1.1. Sistemas de recomendación	1
2. Introducción al Federated Learning	3
2.1. Información general	3
2.2. Fundamentos y Protocolo	4
2.3. Problemas presentes	4
3. Desarrollo	7
3.1. Requisitos del sistema	7
3.1.1. No Funcionales	7
3.1.2. Funcionales	8
3.2. Gestión de riesgos	8
3.3. Especificación del diseño	9
3.3.1. Instalación de los requisitos en el hardware	10
3.4. Tecnologías utilizadas	10
3.4.1. Sistema de recomendación	10
3.5. Consideraciones sobre la implementación	12
3.5.1. Privacidad	12
3.5.2. Seguridad	12
3.5.3. Combinación de modelos	13
3.5.4. Limitaciones técnicas	13
A. Protección de Datos en la Unión Europea y España	17
A.1. Preludio	17
A.2. Legislación	18
A.3. Derechos fundamentales	19

Capítulo 1

Antecedentes y justificación

1.1. Antecedentes

1.1.1. Sistemas de recomendación

Los sistemas de recomendación fueron mencionados por primera vez en los años 90 y han ido evolucionando hasta estar implantados en gran parte de las empresas actuales. Estos sistemas son sistemas de filtrado de información, que se basan en una gran cantidad de datos, tanto del usuario como de los elementos a recomendar, para predecir cuál será el elemento más apropiado para este. Estos sistemas están estrechamente relacionados con el marketing, ya que el objetivo es conseguir recomendar un elemento que sea del agrado e interés del usuario con los datos que se tienen de él, lo que en la mayoría de los casos va ligado al consumo de bienes o servicios.

Hoy en día se usan en multitud de ámbitos, desde las redes sociales hasta las distribuidoras de contenido como Netflix, pasando por compañías de comercio electrónico como Amazon.

A la hora de realizar la recomendación se realizan filtrados de diferente tipo, estos no son más que la forma en la que el sistema busca correlacionar los usuarios con los elementos que estos consumen, compran o ven. Entre los métodos más comunes para relacionar esta información y obtener resultados eficientes se encuentran:

- Filtros demográficos, que recomiendan en función del sexo, edad, país, oficio, . . .
- Filtros basados en contenidos, como Youtube, que recomiendan contenidos similares a los valorados por los usuarios.
- Filtrado colaborativo, que consiste en recomendar al usuario elementos valorados positivamente por usuarios similares a él.

Sin embargo, existen sistemas híbridos que utilizan varias de las estrategias de filtrado anteriores combinadas. Un ejemplo de ello es el mencionado Amazon, que tiene uno de los algoritmos de recomendación más potentes y eficientes actualmente.

Sin embargo, existen sistemas híbridos que utilizan varias de las estrategias de filtrado anteriores combinadas. Un ejemplo de ello es el mencionado Amazon, que tiene uno de los algoritmos de

1. Antecedentes y justificación

recomendación más potentes y eficientes actualmente.

Esto se debe a dos cosas, en primer lugar que cuenta con una gran cantidad de información de los usuarios, tanto su edad, género, país, dirección, rutinas (si tienen Alexa), . . . como los artículos que miran, compran, añaden a la lista, etc. Con todo esto el algoritmo es capaz de ofrecer recomendaciones muy precisas a los usuarios, lo que le da una gran calidad de servicio a la empresa gracias a esto.

De hecho, en Amazon, si queremos revisar las recomendaciones tenemos un apartado propio para ellas al que se puede acceder fácilmente (Fig1.1).



Fig. 1.1: Recomendaciones de Amazon (Fuente: Amazon[1])

Capítulo 2

Introducción al Federated Learning

Es de gran importancia comprender y conocer lo que es el Federated Learning para entender tanto el desarrollo, como la resolución de los problemas y retos que supone su implementación, por eso, en el presente apartado se explicará a conciencia de que se trata esta tecnología.

2.1. Información general

El aprendizaje federado, es una técnica de aprendizaje automático que entrena un algoritmo a través de diversos dispositivos descentralizados, manteniendo siempre la información en cada uno de ellos (Fig2.1). El algoritmo que se busca entrenar en los dispositivos puede ser de cualquier tipo dentro del campo del aprendizaje automático, redes neuronales artificiales, aprendizaje profundo, árbol de decisión, etc. Por lo cual, se puede decir que el aprendizaje federado es una tecnología habilitadora para el entrenamiento de modelos de aprendizaje automático en redes de dispositivos.

Al contrario del aprendizaje automático convencional que reúne toda la información en un mismo computador, el aprendizaje federado busca entrenar un algoritmo en cada uno de los dispositivos que participen en la red, para luego combinarlos y conseguir un modelo de aprendizaje robusto. Los dispositivos que forman parte de esta red son denominados participantes y todos ellos forman la denominada como red de aprendizaje colaborativo. En esta red, todos aprenden de todos sin necesidad de compartir su información, consiguiendo mejorar la precisión y eficacia del algoritmo.

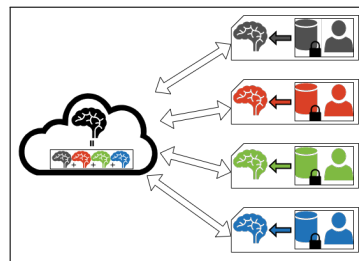


Fig. 2.1: Diagrama de una red de Federated Learning

Esta red permite repartir la carga de trabajo entre todos los participantes, puesto que cada uno se encarga de entrenar su propio modelo. Esto es posible gracias a que cada vez los dispositivos móviles tienen procesadores más rápidos y más potentes, lo que permite que sean capaces de realizar tareas más complejas y pesadas. De esta forma, se consigue que cada dispositivo sea propietario exclusivo de su información y no tenga que compartirla con ningún otro. Además, hoy en día los costes de comunicación son superiores a los de computación, por lo que cuanto más acciones se puedan computar en los dispositivos de los participantes menor será el consumo del entrenamiento del algoritmo.

Sin embargo, debido a estas características propias del aprendizaje federado también sufre de grandes inconvenientes. El hecho de que la red está formada por diferentes participantes la hace heterogénea, con diferentes capacidades de cómputo y diferentes velocidades de conexión entre los distintos participantes, lo que puede incurrir en desconexiones o pérdidas de paquetes durante el proceso de aprendizaje.

2.2. Fundamentos y Protocolo

En general existen dos tipos de entidades en los sistemas de Federated Learning, los propietarios de la información (participantes de la red) y el propietario del modelo (servidor de Federated Learning). Los propietarios de la información entrenan localmente el modelo con la información de la que disponen, mientras que el propietario del modelo agrega los diferentes modelos recibidos de los participantes para mejorar el algoritmo.

La comunicación puede ser llevada a cabo de diferentes maneras, de hecho, hay diseños de protocolos de aprendizaje federado como el desarrollado por los autores del trabajo [2], que lo dividen en 3 fases:

- Selección de los participantes: El servidor elige un grupo de dispositivos conectados para participar en la red.
- Configuración: El servidor se configura en base al mecanismo de agregación definido y envía a los participantes el modelo global.
- Reporte: El servidor recibe la actualización de cada modelo de su respectivo participante. Más tarde los agrega usando el algoritmo elegido.

Además, estos autores definen un parámetro de población con el objetivo de limitar el acceso en caso de que haya muchos participantes, evitando que se conecten a la vez y saturen la red.

2.3. Problemas presentes

Como se ha mencionado antes, implementar el aprendizaje federado implica problemas y costes que hay que asumir y tratar con el objetivo de crear un sistema eficiente y estable.

Cada actualización del modelo conlleva millones de parámetros, además se llevan tantas actualizaciones a cabo como precisión se quiera en el modelo. La gran dimensión de las actualizaciones

puede incurrir en un aumento de los costes de conexión y generar un cuello de botella que puede verse agravado por los participantes, ya sea por la asimetría en las velocidades de internet o por la asimetría en la capacidad de cómputo. Es por eso, que para mejorar el rendimiento y reducir el coste de comunicación se deben considerar varias cosas.

- En primer lugar, todos los dispositivos deben contar con una conexión estable, preferiblemente conexión por cable, o en su defecto conexión inalámbrica por Wi-Fi, descartando por completo todas aquellas conexiones por telefonía móvil.
- En segundo lugar, para minimizar el número de rondas de comunicación se puede realizar computación adicional en los dispositivos para que la agregación global se realice antes.
- También se puede reducir el tamaño de las comunicaciones, ya sea por compresión del modelo, compresión de los datos, o por el uso de una pequeña muestra representativa de estos en vez de enviarlos por completo.
- Por último, se pueden minimizar las actualizaciones de los modelos en base a la importancia de estas. Evitando enviar el modelo global hasta que este no suponga una clara mejora para los participantes.

Capítulo 3

Desarrollo

3.1. Requisitos del sistema

Como bien se ha mencionado previamente, este proyecto trata de adaptar el sistema de recomendación realizado por R.Sánchez [3] a un sistema de recomendación basado en Federated Learning que permita el aprendizaje colaborativo de los participantes. Es por ello que para conocer los requisitos iniciales de diseño del sistema de recomendación se remite al trabajo del autor.

En este apartado se presentarán únicamente los requisitos de la adaptación del sistema y se partirá del trabajo realizado por R.Sánchez. Se presentarán dos tipos de requisitos. En primer lugar los requisitos no funcionales de diseño, las condiciones que debe cumplir la especificación del diseño para cumplir los objetivos del proyecto. En segundo lugar, los requisitos funcionales, las condiciones que ha de cumplir el sistema para ser capaz de funcionar sobre el hardware del que se dispone.

3.1.1. No Funcionales

En cuanto a los requisitos no funcionales se encuentran todos aquellos que se han tenido en cuenta a la hora de plantear el diseño del sistema, es decir, todos los inherentes de la privacidad como patrón de diseño. Por ello el sistema :

RNF1 Mantendrá toda información de los usuarios en sus dispositivos.

RNF2 No expondrá la información de los modelos de inteligencia de los usuarios a otros usuarios.

RNF3 No discriminará entre los modelos de inteligencia artificial a la hora de tomar decisiones.

RNF4 No perjudicará deliberadamente al modelo de un participante.

RNF5 No compartirá información que no sea sintética.

RNF6 No extraerá información de los modelos de los participantes.

RNF7 Combinará los diferentes modelos de los participantes sin acceder a su información.

RNF8 Cumplirá tanto con la LOPD-GDD como con el RGPD (véase ApéndiceA, sección A.2).

RNF9 Respetar los derechos digitales de los usuarios y cumplir con la carta de derechos digitales de España (véase ApéndiceA, sección A.3).

3.1.2. Funcionales

Los requisitos funcionales son básicos en este proyecto para que el sistema sea compatible y ejecutable en el hardware. Por ello, para que el sistema sea compatible con el hardware se han definido los siguientes requisitos:

RF1 El sistema ha de ser ejecutable bajo la arquitectura ARMv8.

RF2 El sistema ha de ser ejecutable bajo la arquitectura x86 y x64.

RF3 El sistema ha de ser ejecutable bajo la arquitectura AArch64.

RF4 El sistema ha de ser ejecutable en Linux.

RF5 El sistema ha de ser ejecutable en Windows.

Además, al margen de los requisitos de compatibilidad también se encuentran los requisitos de recursos, y es que teniendo un hardware poco potente es imprescindible que el software sea lo más óptimo posible para aprovecharlo al máximo. Es por eso que también se definen los siguientes requisitos:

RF6 El sistema ha de ser capaz de entrenar los modelos en un espacio de tiempo razonable, siendo este siempre inferior a los 100 segundos por cada 10 epochs.

RF7 El sistema de recomendación no puede colapsar el dispositivo que lo ejecute,

RF8 El sistema de recomendación debe permitir que el dispositivo pueda funcionar con normalidad durante su ejecución.

3.2. Gestión de riesgos

El motivo de esta sección viene de la definición del modelo en espiral como metodología clave para el desarrollo de este proyecto. Este modelo recoge la identificación y gestión de riesgos como pieza fundamental del ciclo de vida, y en un proyecto con tal complejidad técnica y con tantos dispositivos involucrados, es indispensable tener un plan de acción ante cualquier incidente.

Con tantos dispositivos que gestionar, el proceso de configuración de estos puede llegar a ser algo pesado, y más si alguno de estos falla o se rompe. Si se rompiese o se corrompiese una tarjeta SD de una Raspberry Pi habría que reinstalar y configurar todos los paquetes a mano, proceso que puede ser bastante largo puesto que requiere de interacción humana. Para evitar esto se ha tomado la decisión de crear un script de aprovisionamiento tanto para la Nvidia Jetson Nano como para las Raspberry Pis, de esta manera, en caso de que una tarjeta SD se averiase, bastaría con cambiarla, configurar el protocolo SSH para acceder remotamente a ella y ejecutar el script. Cuando el proceso terminase el dispositivo estaría listo para poder ejecutar el proyecto sin ningún problema.

Las tareas de inteligencia Artificial no son especialmente livianas para un dispositivo, lo que durante un entrenamiento prolongado en el tiempo podría incurrir en un aumento de temperatura de este. Para evitar que los dispositivos alcancen temperaturas elevadas o que sufran cualquier tipo de cortocircuito por su manipulación inadecuada se ha optado por instalarlos en un rack (Fig 3.1).



Fig. 3.1: Rack para Raspberry Pi (Fuente: Amazon[4])

Esta carcasa aparte de proteger los dispositivos viene equipada con ventiladores que ayudaran a que la temperatura de estos sea siempre la adecuada.

Durante el desarrollo se tiene que acceder a estos dispositivos en multitud de ocasiones, para ello se utiliza el protocolo SSH. Sin embargo, al realizarse este proyecto en un ámbito doméstico, existe la probabilidad de que el router sea reiniciado o apagado por cualquier causa externa al proyecto. En tal caso puede que las direcciones IP sean sustituidas y haya que realizar un análisis de la red o acceder físicamente a estos dispositivos para averiguar la IP. Para evitar este proceso se ha instalado el paquete *AVAHI*¹ que permite acceder mediante SSH a las raspberrys sustituyendo la dirección IP por el nombre de servidor de los dispositivos.

Para gestionar los cambios que se irán haciendo sobre el software sin problemas es indispensable contar con herramientas de control de versiones. Estas herramientas permiten gestionar cuándo se han realizado qué cambios y en caso de necesitarse se podrían revertir con facilidad. En este caso, tanto para el desarrollo del proyecto como para el desarrollo de la memoria se utilizará Git como controlador de versiones. Además, se utilizará Github como repositorio de código en la nube, para así poder clonar el repositorio a los dispositivos facilmente.

3.3. Especificación del diseño

Teniendo en cuenta los anteriores requisitos y los objetivos del proyecto la especificación del diseño concretará como se han diseñado las diferentes funcionalidades y como se ha implementado el Federated Learning en el proyecto.

¹AVAHI es un servicio que facilita el descubrimiento de dispositivos en la red local a través de mDNS/DNS-SD.

3.3.1. Instalación de los requisitos en el hardware

3.4. Tecnologías utilizadas

3.4.1. Sistema de recomendación

El sistema de recomendación de R.Sánchez utiliza LightFM² para crear los modelos de inteligencia artificial. Para implementar el aprendizaje federado se ha tenido que modificar gran parte del sistema de recomendación previo y se ha tenido que hacer uso de las utilidades que proporciona LightFM que se van a explicar en los siguientes apartados.

3.4.1.1. Creación del modelo

El paso de creación del modelo es un paso complejo puesto que conlleva la correcta gestión de muchos datos e información. Asimismo, estos datos han de estar correctamente estructurados y contruidos, puesto que LightFM requiere que la información este convertida a matrices dispersas y no tolera elementos vacíos en ellas. Para ello LightFM provee de herramientas de creación de datasets que facilitan la creación de las matrices, de forma que sea más fácil incluirlas en el modelo.

Entre estas herramientas se encuentran:

- *build_user_features(...)* Permite crear la matriz CSR de usuarios y atributos de usuarios.
- *build_item_features(...)* Permite crear la matriz CSR de items y atributos de items.
- *build_interactions(...)* Permite crear las matriz COO de interacciones y las matriz COO de sus correspondientes pesos.

Hay que tener en cuenta que las matrices CSR (Compressed Sparse Row) hacen referencia a las matrices que admiten operaciones matriciales y acceso eficientemente; y que las matrices COO (Coordinate list) hacen referencia a las matrices que soportan modificaciones eficientemente, son generalmente utilizadas para construir matrices.

3.4.1.1.1. Atributos de los usuario Para crear el modelo es necesario, entre otras cosas, disponer de las características de los usuarios. En este caso contamos con multitud de atributos sobre cada usuario: edad, género, nivel educativo, país, cultura de trabajo, perfil PST (Pinball, Shortcut, Thought-ful), barreras, intenciones y confianza.

Para convertir toda esa información del usuario a la matriz CSR que exige LightFM habrá que llamar a *build_user_features(...)* con los IDs de usuario y y sus atributos, formando una lista que tenga listas de los IDs de los usuarios con sus listas de atributos, es decir:

$$\left[\left[userId_1 \quad \left[feature_{11} \quad \cdots \quad feature_{1w} \right]_1 \right] \quad \dots \quad \left[userId_v \quad \left[feature_{v1} \quad \cdots \quad feature_{vw} \right]_v \right] \right]$$

²LightFM es una implementación en python de varios algoritmos populares de recomendación.

Teniendo en cuenta que:

$$\begin{aligned}
 v &\leftarrow \text{Cantidad de IDs de usuario} \\
 w &\leftarrow \text{Cantidad de atributos por usuario} \\
 userId_v &\leftarrow \text{ID del usuario } v \\
 feature_{vw} &\leftarrow \text{Atributo } w \text{ del usuario } v
 \end{aligned}$$

Una vez creada la lista y pasado como parámetro al método, obtendremos la matriz CSR de atributos de usuario.

3.4.1.1.2. Atributos de los elementos Además de los usuarios y de sus atributos, también se ha de disponer de los elementos a ordenar en el ranking, llamados items, y de sus características. En este caso estos items representan las estrategias de persuasión por las que se preguntó a los usuarios en el cuestionario. Sin embargo, al contrario que en el punto anterior, no contamos con tantos atributos sobre estos items, sino que cada estrategia de persuasión cuenta con dos atributos llamados dimensiones. Estos atributos no se encuentran presente en todas las estrategias, lo que da como resultado que haya algunas que tengan dos, una o ninguna dimension.

Para convertir toda esa información de los items a la matriz CSR que exige LightFM habrá que llamar a *build_item_features(...)* con los IDs de las estrategias y y sus atributos, formando una lista que tenga listas de los IDs de las estrategias con sus listas de atributos, es decir:

$$\left[\left[\begin{matrix} itemId_1 & \left[\begin{matrix} feature_{11} & \cdots & feature_{1w} \end{matrix} \end{matrix} \right]_1 \right] \quad \dots \quad \left[\begin{matrix} itemId_v & \left[\begin{matrix} feature_{v1} & \cdots & feature_{vw} \end{matrix} \end{matrix} \right]_v \right] \right]$$

Teniendo en cuenta que:

$$\begin{aligned}
 v &\leftarrow \text{Cantidad de IDs de estrategias} \\
 w &\leftarrow \text{Cantidad de dimensiones por estrategia} \\
 itemId_v &\leftarrow \text{ID de la estrategia } v \\
 feature_{vw} &\leftarrow \text{Atributo } w \text{ de la estrategia } v
 \end{aligned}$$

Una vez creada la lista y pasado como parámetro al método, obtendremos la matriz CSR de atributos de usuario.

3.4.1.1.3. Interacciones Para crear un modelo de LightFM se necesita
 user_features, item_features
 model = LightFM()

3.4.1.2. Ajuste

3.4.1.3. Predicción

3.4.1.4. Evaluación

La evaluación de los resultados obtenidos de las predicciones de los modelos es un apartado fundamental que permite analizar la eficacia de estas predicciones. Además, la utilización de métricas

y técnicas permitirá poder comparar los resultados entre sí para poder demostrar si la predicción es correcta, aceptable o errónea.

3.4.1.4.1. Métricas

3.5. Consideraciones sobre la implementación

En este capítulo se describirán tanto las causas que han llevado a adoptar la previa especificación del diseño del sistema como las razones detrás de ellas. Con el objetivo de ayudar a entender el porqué de las decisiones tomadas se hablará sobre la privacidad, seguridad, la combinación de los modelos y las limitaciones técnicas presentes en este proyecto.

3.5.1. Privacidad

Con el objetivo de no vulnerar la privacidad de los datos, la agregación de los modelos será realizada por consenso sobre usuarios sintéticos. De esta forma, se evitan problemas derivados del robo de datos y las consecuencias tanto legales como personales de este.

Partiendo del principio de que si no circula ningún dato de ningún usuario por la red no se corren tantos riesgos se plantea este sistema de agregación como una alternativa viable a los sistemas tradicionales de ensamblado.

3.5.2. Seguridad

Este sistema está expuesto a los ataques de seguridad derivados de la implementación del Federated Learning. Sin embargo, debido a la naturaleza del algoritmo de consenso, algunos ataques podrían ser minimizados o incluso erradicados.

Un ejemplo de ello es el ataque por envenenamiento. Existen dos tipos de envenenamiento, por datos y por modelo, pero ambos consisten en que un participante de la red, con el objetivo de dañar tanto al sistema como a los participantes, envía modelos de inteligencia artificial (o los datos si es por envenenamiento de datos) debidamente manipulados. En los sistemas de agregación de modelos de inteligencia artificial por ensamblado este tipo de ataque suele ser bastante dañino, ya que es capaz de distorsionar por completo los resultados del modelo final con lo enviado por el atacante.

Sin embargo, debido a la condición del sistema de agregación por consenso, este tipo de ataques no son tan efectivos, ya que el modelo con datos envenenados podría ser ignorado si el método por el que se realiza el consenso es la moda. Con la moda se elegiría el ranking en función de los valores más frecuentes, es decir, el modelo del atacante sería ignorado por presentar predicciones que no se ajustan a ninguno de los demás participantes.

Cabe destacar que con el objetivo de detectar ataques y encontrar posibles modelos maliciosos se podrían descartar del proceso todos aquellos modelos que presenten unas predicciones totalmente diferentes. Se podría analizar la varianza de las predicciones de cada modelo para descartar del proceso a presuntos modelos envenenados.

3.5.3. Combinación de modelos

Debido a que el principal objetivo de este proyecto es el desarrollo de un sistema de recomendación con aprendizaje federado con la privacidad como patron de diseño, la combinación de los diferentes modelos de los participantes ha sido un factor muy importante a tener en cuenta. En el Machine Learning tradicional esta agregación de modelos se producía mediante el ensamblado de modelos. Sin embargo, este proceso no es compatible con este proyecto puesto que para poder ensamblar los modelos habría que compartir información de los participantes de la red.

Para evitar compartir ningún tipo de información que comprometiese la seguridad y privacidad de los participantes de la red de aprendizaje federado pero conseguir que los participantes aprendiesen entre ellos, se optó por compartir los modelos de inteligencia artificial exclusivamente.

3.5.4. Limitaciones técnicas

Debido a que los dispositivos que iban a formar la red iban a ser 4 Raspberry Pis modelo 3b+, el procesado de los datos era un proceso de especial importancia por la *escasa* capacidad de cómputo de estos dispositivos. Estos dispositivos, como se puede ver en el capítulo de especificación del diseño, son dispositivos que tienen cuatro núcleos y 1.4GHz de frecuencia, lo que comparado con un ordenador de sobremesa actual supone una gran diferencia de potencia de cálculo.

Además, esa no es la única diferencia que tienen respecto a los ordenadores de escritorio, las Raspberry Pis funcionan sobre arquitectura ARMv8 y no sobre las tan usadas x64 y x86. Esto implica un gran problema a la hora de instalar los paquetes necesarios para que el proyecto sea ejecutable en estos dispositivos, ya que la mayoría de los paquetes necesarios están pensados para las arquitecturas más comunes (x64 y x86). Sin embargo, se han podido encontrar las versiones funcionales de todos los paquetes para estos dispositivos.

El dispositivo que iba a agregar los datos, la Nvidia Jetson Nano, ha sido más sencilla de configurar puesto que esta funciona sobre arquitectura AArch64, extensión de 64bits de la arquitectura ARM.

Bibliografía

- [1] *Amazon.es: compra online de electrónica, libros, deporte, hogar, moda y mucho más.* es-es. dirección: <https://www.amazon.es/> (visitado 25-04-2021).
- [2] K. Bonawitz y col., "Towards Federated Learning at Scale: System Design," *arXiv:1902.01046 [cs, stat]*, mar. de 2019, arXiv: 1902.01046. dirección: <http://arxiv.org/abs/1902.01046> (visitado 26-04-2021).
- [3] R. Sánchez-Corcuera, D. Casado-Mansilla, C. E. Borges y D. López-de-Ipiña, "Persuasion-based recommender system ensembling matrix factorisation and active learning models," en, *Pers Ubiquit Comput*, mar. de 2020, issn: 1617-4909, 1617-4917. dirección: <http://link.springer.com/10.1007/s00779-020-01382-7> (visitado 24-04-2021).
- [4] *para Raspberry Pi 4 Model B,Raspberry Pi 3 B + Caja con Ventilador de refrigeración y disipador de Calor, Caja de acrílico de 4 Capas Caja apilable Cluster Caja para Raspberry Pi 3/2 Modelo B: Amazon.es: Grandes electrodomésticos.* dirección: https://www.amazon.es/Raspberry-Ventilador-refrigeraci%C3%B3n-disipador-acr%C3%ADlico/dp/B07J9VMNBL/ref=sr_1_2?__mk_es_ES=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=raspberry+rack&qid=1619378660&sr=8-2 (visitado 25-04-2021).

Apéndice A

Protección de Datos en la Unión Europea y España

A.1. Preludio

Ante la llegada de las Tecnologías de la Información y la Comunicación (TIC), la Organización para la Cooperación y el Desarrollo Económicos (OCDE) decidió definir unas directrices el 23 de septiembre de 1980 que regulen “.. la protección de la privacidad y el flujo transfronterizo de datos personales ... ” [1, págs.1]. Este fue uno de los primeros intentos de regular la gestión y utilización de los datos personales.

No llegaron medidas concretas a Europa hasta el 24 de octubre de 1995, cuando el Parlamento Europeo y el Consejo Europeo publicaron la “*Directiva 95/46/CE*” [2] con el objetivo de crear un marco jurídico que garantizase la protección de los datos y la libre circulación de estos. Por eso, en España se creó la “*Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*” [3] más conocida por sus siglas LOPD, que era la encargada de garantizar el cumplimiento de la directiva europea en España.

Ante la ausencia de leyes que garantizaran el cumplimiento de los derechos humanos en internet, algunos autores empezaron a definir los derechos digitales. Una de las primeras declaraciones de derechos fundamentales tecnológicos fue la de Robert B. Gelman, que en 1997 difundió una propuesta de “*Declaración de los Derechos Humanos en el Ciberespacio*”, basada en la Declaración Universal de los Derechos Humanos de 1948.

Sin embargo, aunque el trabajo de Robert B. Gelman fue ampliamente apoyado por una gran comunidad de expertos, no ha sido hasta la entrada en el siglo XXI (cuando las TIC ya han conseguido una gran relevancia en la sociedad) que se ha empezado a atisbar la necesidad de derechos digitales inherentes de vivir en una sociedad tecnológica. Tanto es así, que varios autores empezaron a escribir sobre la necesidad de una nueva generación de derechos humanos que incluyese el campo de la tecnología.

La corriente pro derechos digitales llegó inclusive a la Unión Europea, que en el año 2000 re-

dactó la *Carta de los Derechos Fundamentales de la Unión Europea* [4] en Niza con el objetivo de "... reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos." [4, págs.5]. El problema es que no pasó a ser jurídicamente vinculante hasta el año 2009 junto con el Tratado de Lisboa. Esta carta es especialmente innovadora en cuanto a la protección de datos de carácter personal, puesto que establecía como derecho fundamental la protección de estos en el artículo 8. En este artículo se establecía que además, estos se tratarían de modo leal y con el consentimiento de la persona afectada. Asimismo, la persona afectada tendría derecho a acceder a los datos recogidos, así como a la rectificación de los mismos.

A.2. Legislación

La legislación vigente en Europa cambió radicalmente en el 2016, el parlamento europeo adoptó nuevas medidas para la era digital.

El 5 de mayo de 2016 entró en vigor la Directiva (UE) 2016/680 [5], reconocida como la Directiva sobre protección de datos en el ámbito penal, "... relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos ..." [5, págs.1]. La Comisión Europea define esta medida en su página web [6] como:

"... protege el derecho fundamental de los ciudadanos a la protección de sus datos cuando los utilicen las autoridades policiales y judiciales a efectos de aplicación de la ley. Más concretamente, la Directiva garantizará que se protejan adecuadamente los datos personales de víctimas, testigos y sospechosos de delitos, además de facilitar la cooperación transfronteriza en la lucha contra la delincuencia y el terrorismo."

El 24 de mayo de 2016 el Reglamento (UE) 2016/679 [7], reconocido como el Reglamento General de Protección de Datos (RGPD). "... relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ..." [7, págs.2]. La Comisión Europea define esta medida en su página web como:

"... es una medida esencial para fortalecer los derechos fundamentales de las personas en la era digital y facilitar la actividad económica, ya que aclara las normas aplicables a las empresas y los organismos públicos en el mercado único digital. Además, la existencia de una norma única pone fin a la fragmentación en distintos sistemas nacionales y a las cargas administrativas innecesarias."

Esta legislación no sería aplicable hasta dos años más tarde, el 6 y 25 de mayo de 2018 respectivamente. Dos años durante los cuales cualquier empresa de la unión o cualquier empresa que tenga negocios en la Unión Europea se debía adaptar a la nueva normativa.

El objetivo principal de este reglamento era proteger a las personas físicas en cuanto al tratamiento de sus datos personales y a la libre circulación de estos. Estos datos son de naturaleza sensible, puesto que pueden revelar la identidad de la persona, ya sea mediante el nombre comple-

to, la dirección de su domicilio, el número de tarjeta bancaria, etc.

Entre las cuestiones más relevantes del RGPD destacan:

- La transparencia: obliga a las organizaciones a comunicar a los usuarios el tratamiento que se realiza a sus datos.
- El derecho a la rectificación y borrado: cada usuario tendrá derecho a pedir que se rectifiquen sus datos en caso de ser inexactos. Además, los usuarios tendrán derecho a que las organizaciones borren sus datos y rescindir el consentimiento de tratamiento de ellos.
- Derechos sobre el procesamiento: cada usuario podrá solicitar la limitación de procesamiento de sus datos, así como negarse a que se usen en tomas de decisiones o en perfiles automatizados, aparte, también podrá solicitar que le entreguen sus datos en formato estructurado cuando sea posible.

La directiva sobre protección de datos en el ámbito penal y el RGPD dejaron obsoleta la LOPD española, por lo cual, para adaptarse al nuevo marco jurídico europeo el 7 de diciembre de 2018 entró en vigor la *"Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales"* [8] (LOPD-GDD), acorde con el RGPD.

Esta ley transpone el RGPD europeo a la legislación española, incluyendo medidas como:

- La incorporación del término privacidad desde el diseño, lo que quiere decir que deben elaborarse procesos empresariales teniendo en cuenta la LOPD-GDD desde un primer momento.
- El consentimiento, donde se obliga a las organizaciones a obtener el consentimiento explícito para el tratamiento de datos de las personas, estas personas, además, podrán solicitar la portabilidad de sus datos o la eliminación de los mismos.
- Sin embargo, la LOPD-GDD no se ciñe únicamente a adaptar el RGPD a la legislación Española, fue la primera ley europea de protección de datos en incluir explícitamente los derechos digitales de las personas en los entornos digitales.

A.3. Derechos fundamentales

Como se ha comentado en el apartado anterior, con la entrada en vigor de la LOPD-GDD España se convirtió en el primer país europeo en garantizar los derechos digitales. Estos derechos digitales llegaron en 2018 en el Título X de la LOPD-GDD, titulado *"Garantía de los derechos digitales"*, en respuesta a la Carta de los Derechos Fundamentales de la Unión Europea y a las nuevas medidas del Reglamento (UE) 2016/679 y de la Directiva (UE) 2016/680.

Varios de los derechos recogidos en la LOPD-GDD fueron:

- El derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.
- El derecho a la desconexión digital en el ámbito laboral.
- Derecho al olvido en búsquedas de Internet.

- El derecho al testamento digital.

Este paso adelante por parte del estado español incentivó a que un año después de la entrada en vigor de la LOPD-GDD, el Ilustre Colegio de la Abogacía de Barcelona (ICAB) presentase la *Carta de Barcelona por los Derechos de la Ciudadanía en la Era Digital* [9], apoyada por universidades y entidades de la sociedad civil.

A la vista de la relevancia e impacto del tema, el gobierno español (representado por el Ministerio de Asuntos Económicos y Transformación Digital), se inspirará en la carta del ICAB para redactar la pionera *Carta de Derechos Digitales* [10] de España, que contribuirá con los objetivos ya avanzados en el Título X de la LOPD-GDD. Se prevé que sea aprobada antes de 2022 para la estrategia España Digital 2025.

Esta carta cuenta con 25 puntos de alta relevancia entre los que están los recogidos en el anteriormente mencionado Título X de la LOPD-GDD, y entre otros, algunos de especial impacto en el desarrollo de este proyecto: los derechos ante la Inteligencia Artificial (Derecho XXIII) y el derecho a no ser localizado y perfilado (Derecho V).

El derecho a no ser localizado y perfilado deja claro que cada persona tiene derecho a la *"... libre autodeterminación individual (...) a no ser objeto de localización, ni a ser sometido a análisis de la personalidad o conducta que impliquen el perfilado de la persona"*, además, añade que sólo se podrán realizar *"... tratamientos de información personal con el consentimiento de la persona afectada ..."*.

En cuanto al derecho ante la Inteligencia Artificial expone como primer punto que, en lo que concierne al desarrollo y ciclo de vida de esta, *"Se deberá garantizar el derecho a la no discriminación algorítmica ..."*. Además, en procesos de decisión automatizada las personas tienen derecho a *"Solicitar una supervisión e intervención humana"* o *Impugnar las decisiones automatizadas o algorítmicas"*.

La carta, al no estar aprobada aún, no es legalmente vinculante, por lo que no es de obligado cumplimiento. Sin embargo, deja clara la orientación que van a tomar los derechos digitales en los próximos años.

Referencias

- [1] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, es. OECD, feb. de 2002, ISBN: 978-92-64-19719-0 978-92-64-19639-1. dirección: https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en (visitado 28-03-2021).
- [2] *DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995*. dirección: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES> (visitado 28-03-2021).
- [3] *LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*. dirección: <https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf> (visitado 28-03-2021).
- [4] “Carta de los Derechos Fundamentales de la Unión Europea,” pág. 17,
- [5] “DIRECTIVA (UE) 2016/ 680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016,” es, pág. 43,
- [6] *La protección de datos en la UE*, es, Text. dirección: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (visitado 27-03-2021).
- [7] *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016*. dirección: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=ES> (visitado 27-03-2021).
- [8] M. B. Samper, *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, es, 1.^a ed. Dykinson, sep. de 2020, ISBN: 978-84-13-77085-7 978-84-13-77029-1. dirección: <http://www.jstor.org/stable/10.2307/j.ctv17hm980> (visitado 28-03-2021).
- [9] *Carta de Barcelona por los Derechos de la Ciudadanía en la Era Digital*. dirección: <https://www.icab.cat/export/sites/icab/.galleries/documents-noticies/2019/documento-carta-de-barcelona-por-los-derechos-de-la-ciudadania-en-la-era-digital-21-02-2019.pdf> (visitado 01-04-2021).
- [10] *Carta de Derechos Digitales*. dirección: https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/SEDIACartaDerechosDigitales.pdf (visitado 30-03-2021).

