Towards Real World Federated Learning

**Project Summary**

**TAs:** Debora Caldarola, Eros Fanì

Many data nowadays cannot be used by traditional Machine Learning (ML) approaches because of their sensitive and privacy-protected nature, even if their use could significantly improve our models' performance. A concrete example is provided by medical data: doctors may use the knowledge from a trained AI model, yet patient data cannot be collected because it is inherently private. Introduced by Google, **Federated Learning** is a ML scenario aiming to learn from privacy-protected data without violating the regulations in force. Within a client-server architecture, a server-side global model has to be learnt leveraging the clients’ data, without breaking their privacy. This is achieved by never giving the server direct access to the data and transferring the trained model parameters.

Let us now imagine the following use case. Alice likes traveling and taking many pictures of the places she visits with her smartphone. On the other hand, John is a professional photographer, so he rarely uses his phone and mainly relies on his camera. Martha is an influencer showing Rome to her followers, so her phone is packed with pictures of that city. All of them would like to have access to an AI model able to recognize the place in which their photos were taken. Due to the private nature of their personal pictures, they need a federated scenario. Locally, the model will have access to Alice’s pictures of many places, almost no photos on John’s phone and Martha’s pics from Rome. ***What happens when a model is trained on so differently distributed data?***

In addition, the pictures could be taken during the day, or at night, during sunny or rainy days, *i.e.* with different weather and light conditions, and so on, which make learning harder. That implies additional issues arise when moving towards more realistic scenarios, which have to be explicitly addressed. In this case, ***can the model generalize to different and potentially new visual shifts, i.e. domains?***

Lastly, it is not realistic to assume to have access to labeled data on the client-side, since labeling is costly and often requires domain expertise. ***What happens when the clients’ data is not labeled?***

### Project overview

The goal of this project is to become familiar with the Federated Learning (FL) framework and the issues arising when facing more realistic scenarios.

The project is divided into 2 tracks, distinguished by both task and addressed challenge. You should pick only one of them.

**Track 1** (TA: Debora Caldarola)

* Task: **image classification**. The goal is to learn to distinguish numbers and letters, written by several users having different handwriting.
* Challenges: heterogeneously distributed data and generalization to unseen domains (*e.g.,* night vs day)

**Track 2** (TA: Eros Fanì)

* Task: **semantic segmentation** for autonomous driving.
* Challenges: heterogeneously distributed data and extension to unlabeled data on the client-side.

In both cases, you will be provided with both existing code and federated datasets to start running the first experiments.