RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

INSTITUT FRANÇAIS

ANTONIO HORTA RIBEIRO

From Sweden to France

Project: **Methods for adversarial training**

Research topic: **Informatics**

Swedish Institution: **Uppsala University**

French Institution: **École Nationale Supérieure (INRIA)**

Dates of mobility: **03/03/2023** to **18/06/2023**

Program: **SFVE-A**

PRESENTATION

Antonio Horta Ribeiro is a Postdoctoral Researcher at the System and Control Division of the Department of Information Technology at Uppsala University. He is interested in learning more about the intrinsic behavior of time series, signals and dynamical systems, and techniques for extracting information. This knowledge can be applicable to among others computational electrocardiography and automated ECG analysis. For more information, visit his personal website. He obtained his PhD in Electrical Engineering from the Universidade Federal de Minas Gerais (UFMG), Brazil, in 2020.

ACTIVITIES IN FRANCE

Antonio Horta Ribeiro's main objective at the National Institute for Research in Digital Science and Technology (INRIA) was to develop new methods for adversarial training, since state-of-the-art machine learning models are vulnerable to small input perturbations of adversarial nature. He was hosted by Dr. Francis Bach and his SIERRA project team at the Informatics Laboratory of the Ecole Nationale Supérieure (ENS) that studies algorithms, theory and applications of machine learning. During his mobility, he wrote the paper "Regularization properties of adversarially-trained linear regression", currently under review and affirming the emergence of the convex optimization problem following adversarial training.

He gave a talk entitled "Overparametrized linear regression under adversarial attacks", with ensuing discussion and feedback, mainly with Dr. Bach but also with Dr. Umut Simsekli. He also attended the PhD defenses of Yann Labbé and Rémi Jézéquel (INRIA), and talks from Nisha Chandramoorthy (Georgia Tech), Pierre-Cyril Aubin-Frankowski (INRIA), Ester Mariucci (University Versailles Saint Quentin), David Blei (Columbia University and Columbia Sata Science Institute), and Lawrence Stewart (INRIA).