©M. Denance

02 NOV

12h00 à 13h30

Séminaire CIA : Mohamed Abdalla, Lê Nguyên Hoang and Aurelien Bellet

02/11/2022 : Conflits d'intérêts et désinformation dans la recherche en IA

AJOUTER AU CALENDRIER

Mohamed Abdalla, Lê Nguyên Hoang and Aurelien Bellet sont invités dans le cadre du séminaire Critique de l'Intelligence Artificielle.

This session is based on a recent news in privacy-preserving machine learning. Indeed, a work of scientific disinformation debunking in this field has been done by Lê Nguyên Hoang, who summarized his work in this recent video (https://www.youtube.com/watch?v=IVqXKP91L4E). Moreover, his arguments are supported by a theoretical work, discussing the non-compatibility between high performance and security/privacy, done with his co-authors that led to this publication : 'On the Impossible Security of Very Large Foundation Models' (https://arxiv.org/abs/2209.15259).

First, Mohamed Abdalla will present this paper (https://arxiv.org/abs/2009.13676) discussing conflicts of interests in artificial intelligence public research. Then Lê Nguyên Hoang will present his paper and it will be followed by a technical discussion with Aurélien Bellet.

About the lecturers

- Lê Nguyên Hoang is a mathematics researcher, web video maker and writer. He is also a popularizer in various fields of science and promotes Bayesianism and the emergence of a debate on the ethics of artificial intelligence. After a PhD in game theory, his research focused on security in machine learning, including Byzantine machine learning and collaborative learning. He is the president and co-founder of the Tournesol association, which proposes a collaborative video recommendation algorithm to fight against misinformation. He also co-founded Calicarpa, a company for secure machine learning.
- Aurélien Bellet is a tenured researcher at Inria (France). His current research focuses on the design of privacy-preserving and decentralized machine learning algorithms. Aurélien is serving as area chair for top international conferences in machine learning such as NeurIPS and ICML. He co-organized several international workshops on machine learning and privacy at NeurIPS, CCS and FOCS, as well as the 10th edition of the French pluridisciplinary conference on privacy protection (APVP). He also co-organizes FLOW, an online seminar on federated machine learning with 1000+ registered attendees.
- Mohamed Abdalla is a Principal Investigator in the AI Deployment and Evaluation Lab at Trillium Health Partners. He earned his PhD in Computer Science from the Natural Language Processing Group (Department of Computer Science) at the University of Toronto. His work explores the application of machine learning in healthcare.