Federal University of Minas Gerais
Department of Computer Science

Modeling Differential Privacy and Algorithmic Fairness through the lens of Quantitative Information Flow and Causality

Artur Gaspar da Silva

PhD research proposal presented to the Graduate Program as one of the requirements to apply for the doctoral course.

Minas Gerais, Brazil
November 30, 2024

1 Candidate presentation

My name is Artur Gaspar da Silva, and I'm currently a Computer Science Bachelor student at the Federal University of Minas Gerais, completing the undergraduate course on 2024. Since the second semester at the University, I was enrolled in Scientific Initiation programs under professor Mário Sérgio Alvim, at the Theory Expertise laboratory (T-Rex). My goal on pursuing a PhD is to learn how to effectively become an independent researcher and be able to propose and conduct novel research in the future.

I participated in four projects at T-Rex during my undergraduate course:

1. I developed a Multi-agent model for opinion evolution in social networks under cognitive biases, extending previous work that modeled only Confirmation Bias to model other important cognitive biases, such as the Backfire-Effect and Authority Bias. This resulted in a paper titled "A Multi-agent Model for Opinion Evolution in Social Networks Under Cognitive Biases", published at the International Conference on Formal Techniques for Distributed Objects, and presented at Groningen, at the Netherlands, in June 2024.

2. I developed methods of using concepts from the Quantitative Information Flow framework to model the quantification of information leakage from strategies used to update dynamic secrets. Originally, the QIF framework models static secrets only, but it is known that in some situations an adversary can obtain information about a secret-changing strategy, and thus the developed theory actually extends the capabilities of the QIF framework.

3. I helped preparing classes taught to "Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira" (INEP) on privacy concepts and tools that can be used to protect the privacy of citzens when disclosing aggregated information on the educational census.

4. I participated during one month in a project to model the trade-offs between privacy and fairness in Machine Learning at the french National Institute for Research in Digital Science and Technology (INRIA), at the École Polytechnique de Paris campus. I studied the current scientific literature on these topics and also the feasibility of introducing Causality concepts to model fairness and privacy, and suggested some ideas on possible next steps.