

# Abstract: Should I Trust It With My Data? Capabilities, Limits, and Perspectives of AI Technologies for Privacy

Victor Morel<sup>1</sup>

<sup>1</sup>*Chalmers University of Technology, Gothenburg, Sweden*

## Abstract

It is impossible to miss the AI wave which shakes many aspects of society. This new 'AI-summer' started in the early 2010s with the rise of Deep Learning but gained a new momentum with the popularization of applications based on Transformers Models. AI is now a topic of conversation at a family dinner since it pervades so many aspects of our lives. Such a disruption is not without consequences, and some of these consequences regard the impact of AI on privacy. But what can AI do to privacy: does it enhance it, or undermine it? Is automation always desired and always desirable? Can we even legally introduce AI in all aspects of our lives? What are the considerations one must take to integrate AI technology in privacy-sensitive systems? To address these questions, this talk will take us on a tour of some of my recent research on the matter, including academic publications, a master thesis project, and some other informed opinions. It may however not provide definitive answers to all of them, and rather incite to discuss this important topic.

---

*SPAIML'25: International Workshop on Security and Privacy-Preserving AI/ML, October 26, 2025, Bologna, Italy*



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).