# Privacy in the Artificial Intelligence World: A Comprehensive Review of Current Research

**Nadav Voloch ***

Ariel University, Israel

**Ron Hirschprung**

Ariel University, Israel

## Abstract:

The intersection of artificial intelligence (AI) and privacy presents significant challenges, particularly as AI systems become integral into sectors such as finance, healthcare, and online social networks. This research examines the complex relationship between AI and privacy, emphasizing the need for a clear view of these in different domains. By reviewing over 100 research papers, we categorize privacy concerns across four primary dimensions with the following values: a) Domain (Technological): LLM, ML, NLP, Computer Vision, Speech Recognition, IoT, OSN, D/B; b) Actions: attacks, defense, awareness, vulnerabilities, threats, regulations; c) Approach: Privacy by Design (PbD), Privacy Shell, Hybrid (PbD+Shell), Advisory, PPDM; and d) AI-Privacy relation direction: Harnessing AI to protect privacy, AI as a threat to privacy, AI usage that includes privacy, applying privacy to AI. We also used a novel approach based on Graph Database to optimize the presentation of the results and enable efficient search according to multiple keys, as well as later updates by the reader itself. This study provides a comprehensive taxonomy for understanding and addressing privacy issues in AI, offering insights critical for researchers, policymakers, and practitioners in navigating the evolving landscape of AI and privacy.

## Keywords:

Artificial Intelligence (AI), Privacy, Machine Learning (ML).