Privacy and Artificial Intelligence

Michael Birnhack

Artificial Intelligence technologies consume large amounts of data, including personal data about individuals. The processing, uses, and output of AI technologies also relate to humans and affect their lives. This article examines the interface between AI technologies and privacy. The framework of the discussion is the research paradigm of law and technology, which is keenly aware of the complex connections between the two elements, though both are value-based. The article refers to AI technology as a general name for technological methods for processing data, including personal data, using big data for the purpose of machine learning, to detect general behavioral patterns and then apply them to a specific person. To find out whether and how AI harms privacy, the article examines different phases in the data lifecycle and points to a series of challenges regarding the law. I examine the notice and consent duties, the principles of data minimization and purpose limitation in privacy law, challenges of identification at the stage of collecting the data, but not at the stage of using the technology, and challenges related to data processing and using it for drawing conclusions and inferring predictions about people. The conclusion at present is that privacy laws are by and large prepared to handle AI challenges. But above all, over everything hovers the challenge of power—the power imbalances between data subjects, the information-hungry corporations, and the machine.