MVV347K AI, Law, and Governance

Lecture 3 – AI and data / privacy

ChatGPT banned in Italy over privacy concerns https://www.bbc.com/news/technology-65139406

CAIPD's FTC complaint in the matter of OpenAI https://www.caidp.org/cases/openai/

China's First Facial Recognition Case https://www.chinajusticeobserver.com/a/china-s-first-facial-recognition-case

Focus on GDPR – it introduces new rights for data subjects = new obligations for organisations

Large-scale automated processing of personal data, specifically addressing the use of automated decision-making

Big data analytics (combination of AI, Big Data and machine learning) has the following distinctive features:

a) The use of algorithms in a new way (to find correlations in order to create new algorithms)

b) Opacity of the processing (where deep learning is involved)

c) The tendency to collect all available data

d) Repurposing data (reusing data for a purpose different from that for which it was originally collected)

e) The use of new types of data (new data produced by the analytics rather than being consciously provided by individuals)

Clash with GDPR principles

Guidance on how to explain AI to users, guidance on auditing AI to develop bets practices for data compliance of AI applications

Counterfactual explanations as proposed by Wachter, Mittelstadt and Floridi is one possible approach to improve the transparency and accountability of automated decision-making

Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, Wachter, Mittelstadt and Floridi (2017) uploaded to IS

Article 22 – further interpretation of key terms will be required (CJEU)

Task: Consider the legal and ethical impact of using data generated by the AI expert systems / metadata / inferred data – protection, consent, accuracy, transparency.

Recommended reading: Prof. Dr. Lilian Mitrou, Data protection, artificial intelligence and cognitive services - Is the GDPR "artificial intelligence-proof"?

Application of consumer protection laws

Issue of psychometric testing and targeted advertising

Issue of electoral interference, fake news

There seems to be no active cross-regulatory cooperation between data protection, electoral and media authorities on the national or EU level

The manipulative (re)use of personal data for targeted advertising undermines the sustainability of democratic principles, processes, institutions and rights

Technology companies – neither a platform, nor a publisher – a new category that would create legal liability for content identified as harmful after it has been posted by users

Data trusts

- A legal structure that provides for an independent stewardship of data
- Data is held on behalf of the data subjects and for their benefit
- Potential to align privacy, IPRs and contractual limitations

Recommended reading: 'Data trusts: legal and governance considerations', Queen Mary University of London, BPE Solicitors LLP and Pinsent Masons LLP 2019

EU Data Governance Act https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

Challenging power in data science, Data Feminism by Catherine D'Ignazio and Lauren Klein

The Privacy Advisor Podcast: Carissa Véliz on privacy, AI ethics and democracy

How to address AI and data privacy challenges:

1. Implement user-friendly consent mechanisms that are concise and easily understandable to ensure that users are fully informed about how their data will be used.
2. Develop adaptable strategies for data privacy compliance that can navigate the varying legal landscapes of different jurisdictions while maintaining consistent data protection standards.
3. Enhance diversity in training data and employ bias detection algorithms to identify and address discriminatory patterns in AI models, ensuring fairness and reducing bias.
4. Prioritize cybersecurity measures by employing encryption, access controls, and regular security audits to safeguard sensitive data from potential breaches and unauthorized access.

5. Implement advanced de-identification techniques that not only remove direct identifiers but also consider potential re-identification risks, ensuring that anonymized data remains truly confidential.