LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Ethical and Legal aspects on Human-Technology Interoperability and AI Processing of Emotional Data

A conference on bi-directional influence of AI processing of emotional and bio-data on current and future regulations, 6 June 2023, University of Lapland

Abstracts

When AI gets emotional, does the GDPR apply?

Arno Lodder, Vrije Universiteit van Amsterdam

The talk of the town ChatGPT is sometimes getting emotional. Like when ChatGPT was arguing a human user was not sentient. No matter how emotional it seems, it is not emotions as what we humans consider emotions. ChatGPT seems to be 'selfaware' of that:

"my responses may seem to have a certain tone or emotion, but this is not the result of any emotional influence on my part. Instead, it is due to the way in which language and text can be interpreted and perceived by humans".

So it is all a matter of perception. Obviously, there is more AI than ChatGPT. Over 5 years ago Google's interactive AI ALICE read emotions from your drawings. And ever since Picard published in 1995 Affective Computing, gradually more so-called emotion AI is being developed.

In this presentation I want to discuss the relevance of the GDPR for emotional data processed by AI. That I am working in Amsterdam, and defended my Ph.D exactly 25 years and a day before I give this presentation is data about me. If AI processes this data, who is the data controller, is there one? These are facts about me, but what if the AI tries to analyse what my emotions are related to those facts. That I am arrogant because most people from Amsterdam are, or that I am egocentric because I always talk about myself. Does the GDPR apply to such analyses of AI? And what if AI perceives, and reads from your face your emotions, is the GDPR applicable? These and other questions related to emotional AI and the GDPR are addressed in my presentation.

A Duty of Loyalty for Emotion Data

Woodrow Hartzog, University of Boston

Data privacy law fails to stop companies from engaging in self-serving, opportunistic behavior at the expense of those who trust them with data about their emotions, affect, and other sensitive bodily data. This is a problem. Modern tech companies are so entrenched in our lives and have so much control over what we see and click that the self-dealing exploitation of people has become a major element of the internet's business model. Academics and policymakers have recently proposed a possible solution: require those entrusted with people's data and online experiences to be loyal to those who trust them. A duty of loyalty for emotion data and other sensitive data processing would mitigate the risks of digital opportunism in information relationships. Data collectors bound by this duty of loyalty would be obligated to act in the best interests of people exposing their emotions and online experiences, up to the extent of their exposure. They would be prohibited from designing digital tools and processing data in a way that conflicts with trusting parties' best interests. A duty of loyalty would certainly be a revolution in data privacy and A.I. law. But that is exactly what is needed to break the cycle of self-dealing and manipulation ingrained in our digital tools and our society as a whole.

Talking to strangers. On people-machine communication and the automated detection of online solicitation of children

Hingh, A.E. de, Vrije Universiteit Amsterdam

In most European countries, online grooming (i.e. the online solicitation of children for sexual purposes) is a criminal offence. For the purpose of detecting online grooming, investigative authorities may use A.I. (chatbots) impersonating minors to catch potential groomers in online conversations. A recent Dutch legislative proposal will also prohibit mere online sex chatting with minors (i.e. grooming without proposing a meeting). In tracking down this offence, too, the police may use virtual decoy teenagers to establish (potentially punishable) sexually charged conversations with minors. Finally, in a recent proposal by the European Commission, ISPs and providers of interpersonal communication services will be required to use AI (language recognition software) to scan all online communications to detect solicitation of children. The "linguistic indicators" that they track down will be stored in a new EU-centre and will be used to train the A.I. even further. Clearly, A.I. is given a pivotal role to combat the online solicitation of children, as a speaker, eavesdropper and collector of suspect language. In my contribution I will address the consequences of this type of regulation in which artificial intelligence, emotion and speech all play a crucial role.

Damage caused by Emotional AI – Do existing and planned liability rules provide sufficient protection?

Béatrice Schütte, University of Lapland

Emotionally intelligent AI can process the most personal and intimate information. When this is not handled with utmost care, it can cause discrimination, stigmatization, it can violate a person's privacy and cause other infringements of fundamental rights. This is particularly relevant in relationships with significant power asymmetry, such as that between an employer and an employee or a public authority and a citizen. Often times, the damage inflicted upon individuals is not tangible, meaning that it does not result in actual physical injury or damage to items of property. Still, it can cause serious distress to individuals. The purpose of this contribution is to examine whether existing and planned liability rules provide affected parties with sufficient protection. Relevant frameworks will be the GDPR, the proposed Directive on AI Liability and national civil liability laws. Special focus will be on the recoverability of immaterial harm. To date, many national laws – and courts – are reluctant in providing compensation for non-material harm. The question is whether this reluctance is still appropriate considering the significant risks AI can pose for fundamental rights and other immaterial interests.