Artificial intelligence in criminal law

The use of artificial intelligence (AI) in a broad range of areas is the subject of wide debate at EU level. Establishing an EU approach to AI is one of the European Commission's digital priorities, as illustrated by the proposal on an artificial intelligence act. Despite the great opportunities they offer, AI applications can also entail significant risks to people's fundamental rights. At the October I plenary session, the European Parliament is due to debate an own-initiative report on the use of AI by the police and judicial authorities in criminal matters.

Background

AI applications in the area of security and justice have the potential to facilitate the work of police and judicial authorities and to enhance security and the functioning of justice systems. They could arguably improve suspect and victim identification, crime prevention and risk assessment. However, the use of AI for law enforcement and judicial purposes can have adverse effects, undermining fundamental rights, such as the right to non-discrimination, the right to protection of personal data and to a private life, the right to freedom of expression, and the right to a fair trial. Facial recognition technologies, predictive policing tools and tools to assess the risk of someone reoffending pose particular concerns, given the increased risk of reproducing bias and perpetrating discrimination. AI applications also carry security risks, as they can be both vectors and targets of cyber-attacks, and can be abused by criminals for malicious purposes.

European Commission and Council

The EU institutions have been progressively shaping the EU's AI agenda with several policy documents. The Commission's work on AI has translated into the 2018 AI strategy for Europe, the 2020 white paper on AI and a recently updated coordinated plan on AI. In April 2021, the Commission unveiled a legislative proposal for an artificial intelligence act. The proposal provides for a risk-based classification of AI systems. AI systems for justice and law enforcement are considered 'high-risk' and should comply with strict requirements (conformity assessment, transparency, human oversight). Council too has recognised the specific fundamental rights requirements arising from AI use in law enforcement, while emphasising AI's potential to improve crime prevention, investigation and prosecution. In its December 2020 conclusions on internal security, the Council set an objective that, by 2025, law enforcement authorities should be able to use AI technologies in their daily work, 'subject to clear safeguards'. On AI in the justice sector, Council has advocated the need for human decision-making and stressed the need for effective legal remedies to ensure the right to a fair trial, presumption of innocence and the right of defence.

European Parliament

In recent years, Parliament has expressed its views on AI extensively in multiple policy contexts, for instance in its resolutions on the fundamental rights implications of big data in 2017 and on civil and military uses of AI in 2021. The own-initiative report of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) looks into the promise and risk of AI in the law enforcement and criminal justice context. The report insists on the need to respect the EU fundamental rights *acquis* in full and to build core principles into the AI life cycle (algorithmic explainability, transparency, traceability, compulsory fundamental rights impact assessments, audits, etc.). Stressing the importance of security and privacy by design and human oversight of AI applications, it calls for a ban on the deployment of facial recognition systems for law enforcement purposes, on any processing of biometric data that leads to mass surveillance in public spaces, as well as on the AI-enabled scoring of individuals and the use of AI for proposing judicial decisions.

Own-initiative report: 2020/2016(INI); Committee responsible: LIBE; Rapporteur: Petar Vitanov (S&D, Bulgaria).

EN