Assessment of EU Legislation in the Digital Field

Anna Pingen

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Anna Pingen
Researcher
Max Planck Institute for the Study of Crime, Security and Law

ISSN: 1862-6947
https://eucrim.eu

On 31 January 2022, the EP published a scientific study on the "Identification and assessment of existing and draft EU legislation in the digital field". The study was conducted at the request of the special committee on Artificial Intelligence in a Digital Age (AIDA). It provides an overview of digital legislation and possible regulatory gaps, as there has been a phase of great legislative production in the last few years and an even faster pace of development in digital technologies and their applications. The study aims to:

- Give a systematic overview of existing and upcoming digital regulations and directives;
- Analyse and systematise the interplay between the most important legislative acts and their coherence;
- Identify regulatory gaps.

In so doing, the study has identified gaps in the European Commission proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) adopted on 21 April 2021 (→ eucrim 2/2021, 77).

According to the study, the Artificial Intelligence Act (AI Act) did not take into account social scoring, biometric identification systems, and AI systems for military-purposes. The study also criticised that it is not clear to what extent high risks have been consistently identified throughout all relevant regulations and whether the high-risk category should lead to the application of strict liability regimes in any event. The interplay between the AI Act – as the core component of the AI regulatory framework – and other legal acts might hinder the development of a flawless regulatory framework for AI in the EU. This is especially true with regard to the interplay between the AI Act and the General Data Protection Regulation (GDPR), because more clarity in the AI Act with regard to the processing of personal data is needed.

Furthermore, the interplay between the liability exemption – under the e-Commerce Directive – and the intensive use of algorithmic decision-making in content moderation, notice and removal, complaint-handling, and conflict solving is creating additional points of friction. This raises the question of whether the poor performance of algorithmic voluntary measures in failing to detect (illegal/inappropriate) content should be interpreted as explicit operator knowledge, triggering a duty to react and a resultant liability.

The study also stressed problems regarding the interplay between AI and cybersecurity, as AI might aggravate cybersecurity risks by rendering cyber-attacks more easily targeted and more destructive, on one hand. On the other hand, AI systems may also enhance the effectiveness of preventive measures against cyber-attacks serving as a shield against cybersecurity breaches.

Ultimately, there are potential problems regarding the implementation of the Open Data Directive in relation to the proposed Data Governance Act, in the Database Directive, in the P2B Regulation, in the Digital Services Act (DSA), and in the Digital Markets Act (DMA). Overall, coherence and simplicity has been overlooked in the building of a European regulatory system for the digital domain, according to the authors of the study.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union