TechSonar Report 2022-2023

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle

Deputy Head of Section
Academy of European Law

Published in
2022, Vol. 17(4) eucrim pp 238 – 239

ISSN: 1862-6947

https://eucrim.eu

In September 2021, the European Data Protection Supervisor (EDPS) launched the foresight-related project called "TechSonar". With TechSonar, the EDPS hopes to be able to better determine which technologies are worth monitoring in order to be better prepared for a more sustainable digital future in which the protection of personal data is efficiently guaranteed (→ eucrim news of 3 June 2022). In November 2022, the EDPS published the second edition of its TechSonar Report for the years 2022-2023.

In the first chapter, the 2022-2023 report describes the methods applied to conduct such a foresight-related analysis and which emerging technologies were selected for the report:

- Fake news detection systems;
- The metaverse;
- Synthetic data;
- Federated learning;
- Central Bank Digital Currency (CBDC).

For each of these technologies, possible positive and negative impacts on data protection are outlined.

Regarding fake news detection systems, negative impacts projected by the report are, for instance, error rates in the accuracy of applied algorithms and an increase in automated decision-making. Positive impacts include raised awareness and media literacy at the consumer level, with a corresponding effect on data protection, as well as reduced defamation of individuals through effective fake news detection.

Looking at the metaverse, the report finds a series of negative foreseen impacts for data protection such as deeper profiling and constant monitoring, especially of special categories of personal data like physiological responses, emotions, and biometric data.

For synthetic data - artificial data that is generated from original data and a model that is trained to reproduce the characteristics and structure of the original data – the report finds positive potential technological impacts to enhance privacy and to improve fairness through less bias, depending on the quality of the original data on which the model is based.

Issues identified with regard to federated learning (i.e. the development of machine learning models where only model parameters are shared between the parties instead of entire datasets) concern the efficiency of communication and synchronization between the devices, in order to ensure that training tasks will work within a heterogeneous set of devices and address risks concerning data heterogeneity and privacy leaks.

Lastly, in the field of Central Bank Digital Currency (a new form of money that exists only in digital form), positive future impacts on data protection include expectations for more control over personal data and

security as well as enhanced possibilities for anonymity throughout the payment process. Concerns include the fear that the concentration of data in the hands of central banks could lead to increased privacy risks for citizens, that wrong design choices might worsen data protection issues involving digital payments, and that lacking security might turn into severe lack of trust on the part of users.

For all technologies, the report provides dashboards offering figures, statistics, and information on relevant documents, authors, organizations, and projects as well as heatmaps for numerous countries.

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