FINAL REPORT IED Webinar 29.03.2021

Big data in Europe: Are Privacy and Freedom under threat?

In recent years, the term "Big Data" has started to be used extensively in relation to the digital future of Europe. But what is actually meant by "Big Data" and what challenges does it raise for society in general and for Democracy and Politics in particular? What is the balance between the great value it could create in sectors like healthcare or smart cities, and the downsides of disinformation that could undermine democracy?

Panelists, Quentin Jardon, author of the investigation "Belgian Big Brother," Ioan-Cosmin Mihai, Cybercrime Training Officer at European Union Agency for Law Enforcement Training and Hubert Marcueyz, Business Analyst with Orion Health France gathered online to discuss these issues.

An audience poll examined the question "What makes data big?". Both audience and panelists agreed that big data starts with the accumulation of personal data and continues with the possibilities that having access to such big amounts of data offers.

From that consensus, the panel examined the risks posed by creating these huge reservoirs of, often, personal data. Specifically, data theft, and the unethical use of personal data. Throughout the panelists' contributions, there was consensus that personal data had to be stored securely, but panelists pointed out that some companies lacked the technical know-how to do this.

Data consolidation emerged as a concern, with fears that too few organisations control too much of the data.

Mihai explained that one of the problems in keeping data safe stems from the three v's: Volume velocity, and the variety of different data types involved. Tools such as strong encryption should be used for sensitive personal data.

Marcueyz pointed out that in the case of Personal Health Data, data theft is more often the problem rather than improper or unethical use. According to Marcueyz, "this is both at the same time a source of concern and a reason to be optimistic: Source of concern because the organisations who are responsible for taking care of our personal health information do not have the tools or the weapons to face such attacks as hacking and data theft. But also a reason to be optimistic because it means that our legislators have succeeded in preventing the development of highly lucrative uses of our personal health information that would most likely be unethical."

This led to a discussion on the undeniable benefits of big data. During the Covid19 pandemic, we saw how Big Data could provide solutions. Panelists considered the possibility of a so-called "data donor card" that would allow citizens to declare for which purposes, how and for how long they would allow their data to be used – generally for the public good.

There was general consensus that education and training are needed so that data processors know what they can actually do with it. While the general public needs to be informed about their rights over their own data.

Jardon urged people to think before handing over their data: does the company or entity concerned *really* need access to it? If not, why share that information? The principle of data minimisation is something everyone should understand.

When it comes to risk management, the panel concluded that the bigger the risks, the stronger the law should be so we have to set the ground rules for what organisations can and cannot do.

Marcueyz added that he would like to get insights from the so-called digital natives themselves to feed into public government administrations.

All agreed that Big Data can help us better understand the citizens, the local communities and political movements, but can also be used for ill – to manipulate people, blackmail them, or threaten companies with ransomware – so strong safeguards are necessary, now more than ever with the explosion of AI.

By Jennifer Baker

Moderator of the event