PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Issues and gaps analysis in the context of ICT research and innovation

SECURITY AND CYBERSECURITY

Identified issues and gaps

1) **Definition of Security and Cybersecurity**: The ambiguity of the term security and the difficulty or impossibility to achieve consensual definitions of security causes related legal uncertainties.

2) **Security over privacy?** The complexity of the relation between privacy and security and the manifold impacts of this relation on the individual enjoyment and exercise of human rights and on shaping democratic and societal development requires broad debates and political dialogue.

3) **Conflict between stable principles and "liquid" situations**: Political developments in which stability provided by written or unwritten law is neglected or losing in importance weaken the meaning and the weight of existing legislation and rules.

4) **Surveillance effects on humans**: The risks of surveillance are manifold. The issue does not only affect individuals' privacy: the chilling effect may also challenge society by threatening fundamental rights such as the freedom of speech, of assembly and association.

5) **The dominance of big US companies**: Big US based tech companies not only dominate ICT markets but they also dominate research in the field of AI. This might lead to a corresponding dominance in AI products in the future.

6) **Information and power asymmetries**: Power asymmetries caused by unequally distributed information or unequal access to information raise several issues, ranging from potential competitive advantages to losses of autonomy and sovereignty.

7) **Future impacts on democracy**: Individual freedoms, social cohesion, democratic achievements and traditions are at risk. The multitude of threats and the magnitude of issues at stake calls for strong interventions to stop and reverse the antidemocratic impacts of existing and future ICTs.

PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Issues and gaps analysis in the context of ICT research and innovation

SECURITY AND CYBERSECURITY

Identified issues and gaps

8) **Freedom of expression**: Freedom of expression is a central building block of democracy; measures against the abuse of new media for hate speech or the distribution of fake information are endangering this freedom.

9) **Biometrics and ICT for emotion detection**: Biometric analysis based on audio-visual data is often opaque for data subjects. This may lead to discriminatory treatment based on the analysis results, of which affected persons may not even be aware of.

10) **AI and Security**: Decision-making process of AI is usually based on complex mathematical algorithms, making it difficult or impossible to obtain explanations understandable by humans.

11) **AI for predictive policing**: Using predictive policing technologies threatens to undermine the presumption of innocence and, therefore, can disrespect human dignity as well as fundamental rights of individuals.

12) **Security standards for IoT devices**: Security standards for IoT devices are largely a legal gap. No mandatory requirements for IoT security exist; at least not as long as no personal data are used.

13) **Insufficient guidance to participants in open science**: The current governance of open science and particularly open access to scientific research data in Horizon 2020 provides insufficient and misleading guidance to researchers on how to deal with personal data.

14) **Sharing of personal data in open science** fails to be considered to its full potential: how to share personal scientific research data is currently not sufficiently understood. Legal mechanisms for such sharing are missing.

PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Issues and gaps analysis in the context of ICT research and innovation

SECURITY AND CYBERSECURITY

The content of these fact sheets comes from the "Issues and gaps analysis on security and cybersecurity in the context of ICT research and Innovation", realized in 2020 by the Oesterreichische Akademie der Wissenschaften for PANELFIT.

Click here to access the whole document:
https://www.panelfit.eu/wp-content/uploads/2020/11/D41-Issues-and-gap-analysis-on-Security-and-Cybersecurity-ELI-in-the-context-of-ICT-research-and-innovation.pdf