PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Issues and gaps analysis on Security and Cybersecurity”

Context and workflow

Objectives of the Security and Cybersecurity Pillar

- To explore the ethical and human rights issues related to R&D, implementation and use of existing and future ICT as surveillance/security technologies, in particular to analyse how security IT can be designed to respect ethical requirements and human rights.
- To examine the mutual relationships between security, cybersecurity and human rights, taking into account that data privacy is an essential element of cyber security and privacy in general is an essential element of human rights protecting individuals against state powers.
- To explore how evidence-based security policies and measures or the involvement of civil society organisations can contribute to ethically compliant security technologies, respectively reduce the technology fix and resulting human rights infringements.
- To development practical guidelines to overcome ethical tensions and potential human rights infringements in relation to security and cybersecurity policies and measures and to develop recommendations for corresponding amendments of regulatory frameworks in the EU.

How did we derive our issues and gaps I

Expert Workshop on Ethical and Legal Challenges of New ICT and Security/Cybersecurity with three sets of questions

1) Ethical and legal challenges of future ICT

- What are the most challenging ethical and legal issues raised by the use of current ICTs in the context of inner security?
- What are the most challenging ethical and legal issues raised in the context of cybersecurity?
- Taking a look into the future: how will these issues evolve in view of future capabilities of ICT; what new challenges to expect from next ICT generations?

How did we derive our issues and gaps II

2) Gaps and open issues in existing legal frameworks

- Which of the identified challenges are in principle covered by existing frameworks, but not effectively enforced?
- Which issues are not (or not adequately) addressed by existing regulations, standards or codes of conduct?
- Do existing regulations even create or reinforce ethic issues resulting from the use of ICT in the context of security and cybersecurity?

3) Ways to fill gaps and address open issues

- What measures would you recommend to close the gaps and to foster an ethically compliant use of ICTs in the context of security and cybersecurity?
- Which instruments would you suggest and on which level should they be implemented?
- Which amendments, extensions or new regulations would you suggest to cover (also) capabilities of future ICTs?
- How should R&D be managed and controlled to guarantee or support ethically compliant ICTs in the future?

The raw material from the security/cybersecurity workshop

More than 150 challenges, gaps and issues identified by the participants

Preliminary clustering and prioritisation at the workshop

Transferred into topics of the Critical Analysis I

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.

Topics II

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 also weaken the meaning and the weight of existing legislation and rules.

4) Surveillance effects on humans

The risks of surveillance are manifold. It does not only affect individuals’ privacy, the chilling effect may also change society by threatening fundamental rights such as the freedom of speech, of assembly and association.

Topics III

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.

Topics IV

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.

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.

Topics V

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 about.

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.

Topics VI

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.

Topics VII

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.

Outlook major next steps

Operationalisation of D4.1:

- Further input for “D5.1 Guidelines on Data Protection ELI in ICT Research and Innovation” and for “D5.4 Code of Conduct for Responsible Research and Innovation” in form of practical guidance to ICT research

- Separation of issues and gaps that need to be addressed on the regulatory or policy making level (input for “D5.3 Report on the Governance of ICT data protection ELI”, “D5.5 Citizens Info Pack” and “D5.6 Handbook for Journalists”)

PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

www.panelfit.eu

Funded by
EU H2020
Research
and
Innovation
Programme
G A 788039

info@panelfit.eu

@PANELFIT

PANELFIT.NEWS