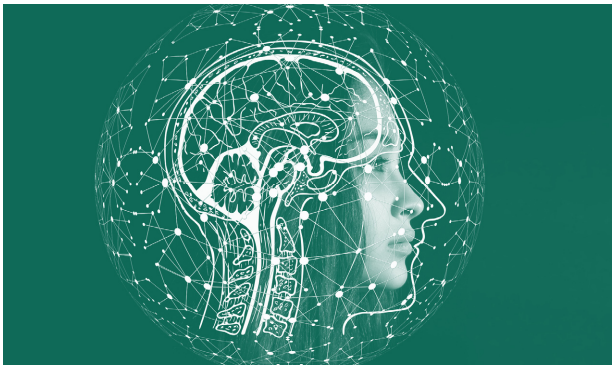
# DO NEW TECHNOLOGIES NEED NEW LAWS?

## IN BRIEF

- Information and communication technologies (ICT) are progressing rapidly and pose a number of major challenges for policy-making and regulation.
- ICT are both a prerequisite for and a threat to security. Establishing security and protecting privacy and civil liberties can best be described as a symbiosis that is not always free of conflict.
- The impact can be felt at individual but also on a global level. As a result, approaches to solutions must also be pursued and developed at all levels.

## WHAT IS IT ABOUT?

Information technologies, such as artificial intelligence (AI) systems or mobile networks, are becoming increasingly more powerful and play an essential role in more and more work spaces and private spheres. With such rapid development, however, how can crucial ethical and legal requirements be taken into account where the development and use of ICT (e.g. in particular in the area of surveillance technologies) is concerned? Policymakers and regulators, too, are confronted with ever-new issues and questions in this area. Where are existing regulations sufficient, and where do new rules need to be developed and implemented? Which recommendations and guidelines need to be updated to enable ethically compliant use of surveillance technologies? Can the huge amounts of data generated by the use of ICT (e.g. social networks) be exploited for security purposes without violating ethical values or fundamental rights? How can actual or perceived conflicts between privacy and security be resolved? These are complex questions, especially when taking into account that privacy and data protection are prerequisites for (cyber)security. Moreover, the protection of privacy is also a central element of human rights, which are essential to provide protection against the abuse of state and economic power.Amongst other topics, the PANELFIT project investgated problems associated with the use of ICT for security purposes.



ICT as surveillance and security technology: Ethical problems because of insufficient regulation?

Key questions were: Are existing regulations, such as the General Data Protection Regulation (GDPR), strong enough? Are existing legal provisions sufficiently enforced? What new measures or amendments are needed in dynamic fields such as AI? Can regulation even create ethical problems or exacerbate them, e.g. when trying to curb fake news by outsourcing censorship to private companies? The aim was to propose measures that make it possible to use ICT for security or surveillance purposes in an ethically sound manner. The use and development of technologies in line with fundamental rights and European values are paramount. In this context, it is also essential to design and implement R&D programmes in such a way that they result in ethically acceptable technologies that can be used in accordance with fundamental rights.

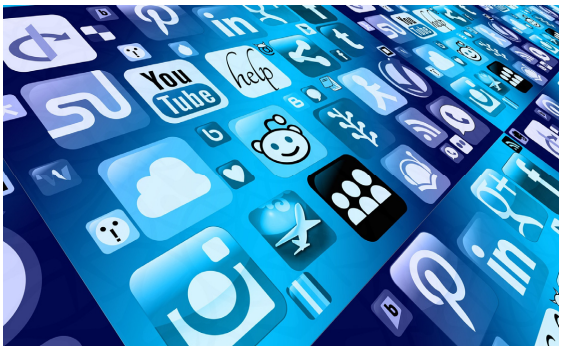
## BASIC DATA

| | |
|---|---|
| **Project title:** | Participatory Approaches to a New Ethical and Legal Frame-work for ICT (PANELFIT) |
| **Project team:** | Čas, J., Krieger-Lamina, J., Peissl, W., Schaber, F. (in an int. consortium) |
| **Duration:** | 11/2018 – 04/2022 |
| **Funded by:** | EU Horizon 2020 |
| **Website:** | www.panelfit.eu |

# KEY RESULTS

"Security" is an ambiguous term. The many facets of security give rise to legal uncertainty and may tempt absuse. The relationship between privacy and freedom on the one hand and security on the other is not an antagonistic one. For democratic societies to flourish, last, and be sustainable, both must be guaranteed. This balance is in danger of being lost.

Next-generation communication technologies, such as 6G networks, combined with new AI-based analytics, offer much more accurate and comprehensive surveillance capabilities that can overcome physical barriers such as walls. Nevertheless, there is a threat that power imbalances between individuals and governments or private companies will increase further. But the states themselves are also affected.




The dominance of global corporations, especially US companies, in new ICT reduces the sovereignty of European states.

Social networks are abused to manipulate citizens, influence election results, and destroy social cohesion. They endanger the existence of democratic societies. Moreover, algorithm-based censorship in private hands, established as a countermeasure, constitutes a further threat to freedom of expression and democratic debate.

Individual technologies or applications raise serious ethical questions. Examples include algorithms for the recognition of emotions and the use of AI for security-related decision-making or predictive policing. Human dignity is violated when people are subjected to procedures or decisions based on non-transparent or inexplicable technologies. Predictive processes, in turn, contradict the principle of the presumption of innocence.

# WHAT TO DO?

**Complex challenges can often be overcome with simple but consistent and rigorous responses. However, their implementation requires radical re-thinking and strong commitment.**

- The continuation of democracies is a central prerequisite for security. If democracies are to last, they must take themselves seriously. That means ensuring that principles and values are consistently defended and that laws are properly implemented and enforced.
- Adherence to principles also means turning away from the usual practice of first responding to conflicts between new technologies and existing regulations by calling for legal adjustments.
  If fundamental rights are to stay, technologies must be adapted to them, and not the other way round.
- Security also has economic dimension.
  The consequences of the COVID-19 pandemic, and especially the war in Ukraine, clearly show how important it is to be able to fall back on production capacities and resources of the European Union (EU). This also applies to the field of ICT in order not to be dependent and susceptible to any actual or potential blackmail.
- Risk-based regulation, as included in the draft for an EU AI Act, is not sufficient. Only clear guidelines can help to minimise risks that are not yet known.

## FURTHER READING

Čas, J. (2019). Issues and gap analysis on security and cybersecurity ELI in the context of ICT re-search and innovation (PanelFit Deliverable 4.1) (61 pp.). Vienna
*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*

## CONTACT

**Johann Čas**
**Email:** *tamail@oeaw.ac.at*
**Phone:** +43 1 51581-6582

IMPRINT: Owner: Austrian Academy of Sciences; Legal person under public law (BGBl. 569/1921 i.d.F. BGBl. I 130/2003); Dr. Ignaz Seipel-Platz 2, A-1010 Vienna; Editor: Institute of Technology Assessment (ITA); Bäckerstraße 13, A-1010 Vienna; *www.oeaw.ac.at/ita/en*. | Frequency: The ITA Dossiers are published irregularly and publish the research results of the ITA. The ITA Dossiers are published in print in small numbers only and are made available open access to the public via the Internet portal "epub.oeaw": *epub.oeaw.ac.at/ita/ita-dossiers* | ISSN: 2306-1960 |  ITA Dossier no. 67en October 2022 |
*epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier067en.pdf*.