Participatory Approaches to a New Ethical and Legal Framework for ICT

PANELFIT

Project Agreement No: 788039

D4.1

Issues and gap analysis on security and cybersecurity ELI in the context of ICT research and innovation

Dissemination level

PU	Unrestricted PUBLIC Access – EU project	X
PP	Project Private, restricted to other programme participants (including the Commission Services) – EU project	
RE	RESTRICTED, restricted to a group specified by the consortium (including the Commission Services) – EU project	
CO	Confidential, only for members of the consortium (including the Commission Services) – EU project	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Document Information

Grant Agreement n°	788039	
Project Title	Participatory Approaches to a New Ethical and Legal Framework for ICT	
Project Acronym	PANELFIT	
Project Coordinator	UPV/EHU	
Document Responsible Partner	OEAW	johann.cas@oeaw.ac.at
Document Number	D4.1	
Document Title	Issues and gap analysis on security and cybersecurity ELI in the context of ICT research and innovation	
Dissemination Level	PP	
Contractual Date of Delivery	Month 11 (30 September 2019)	

Partners involved in the Document

N°	Participant organisation name (short name)	Acronym	Check if involved
1	Universidad del País Vasco/ Euskal Herriko Unibertsitatea	UPV/EHU	X
2	Fonden Teknologiradet	DBT	
3	Vrije Universiteit Brussel	VUB	
4	Oesterreichische Akademie der Wissenschaften	OEAW	X
5	Goethe Universität. Frankfurt am Main	GUF	X
7	European Citizen Science Association (ECSA)	ECSA	X
8	European Network of Research Ethics Committees	EUREC	X
9	Consejo Superior de Investigaciones Científicas	CSIC	X
10	Centro per la Cooperazione Internazionale/ Osservatorio Balcani Caucaso Transeuropa	CCI/ BCT	
12	EVERIS SPAIN, S.L.U.	EVERIS	X
13	Unabhängiges Landeszentrum für Datenschutz AöR	ULD	X

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

Content

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. *This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Executive Summary

This section of the document elaborates issues and gaps related to security and cybersecurity in ICT research and innovation. A major input to this analysis was derived from the Expert Workshop on Ethical and Legal Challenges of New ICT with regard to Security/Cybersecurity held on 4th June 2019 in Bilbao, Spain. Seven external experts from Austria, the Czech Republic, France, Hungary, Spain, and the UK identified, in collaboration with participating members from the PANELFIT consortium, more than 150 ethical and legal challenges of new ICT, as well as gaps and issues in existing legal frameworks. In the context of PANELFIT in general, "gap" is defined as a missing regulation, while "issue" is related to a current regulation that needs further clarification or resolution of conflicts. In the context of this report on security and cybersecurity, in some cases, these terms are used in a wider sense as a number of challenges and concerns identified and discussed at the expert workshop are related to matters beyond legislation, connected for instance to global political trends or economic relations.

The objective of the analysis at hand is addressing the main concerns raised and discussed during the workshop. Additional topics, which were identified at later stages, were also included if regarded as relevant for the addressees of the critical analysis.

The following issues and gaps are analysed in this report:

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 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.
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.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

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 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.
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.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

1 Introduction

This document – Deliverable 4.1 – is entitled "Issues and gap analysis on security and cybersecurity ELI in the context of ICT research and innovation". It contains the Issues & Gap Analyses conducted within WP4 of the PANELFIT project, addressing security and cybersecurity ELI (Ethical and Legal Issues) in relation to ICT research and innovation. A major input to this analysis was derived from the Expert Workshop on "Ethical and Legal Challenges of New ICT with regard to Security/Cybersecurity" held on 4th June 2019 in Bilbao, Spain. Seven external experts[1] from Austria, the Czech Republic, France, Hungary, Spain, and the UK identified, in collaboration with participating members from the PANELFIT consortium, more than 150 ethical and legal challenges of new ICT, as well as gaps and issues in existing legal frameworks. In addition, the experts suggested measures to fill identified gaps and solve open issues. This large number of identified topics reflects the complexity of matters inherent in security, cybersecurity, of future developments of ICT and their mutual interdependency. In subsequent steps during the workshop, the individual topics were clustered and prioritised by the participants. The last two topics included in this analysis have not been derived from the workshop but have been identified as relevant by members of the PANELFIT consortium; addressing issues and gaps related to open science in general they are related to ICT research and innovation beyond the scope of security and cybersecurity.

Main objectives of the Security and Cybersecurity Pillar of PANELFIT (WP4) are to provide answers to the following three topics:

- How can ethical issues and requirements be incorporated into R&D on surveillance/security technologies? What recommendations and guidelines are necessary for an ethically compliant implementation and use of surveillance technologies?
- Can the massive amount of data generated by ICT in general, including social networks, be used for security purposes in an ethically acceptable and human rights compatible manner? What limitations need to be respected, which regulatory and technical safeguards need to be implemented to avoid misuses?
- How can the alleged trade-off between privacy/liberty and security be resolved, considering that data privacy is an essential element of cybersecurity and privacy in general is a critical element of human rights protecting individuals against state powers?

At the Bilbao workshop the experts were asked to provide answers in three subsequent sessions devoted to identify challenges of future ICT, to discuss open issues and gaps in existing regulations and to develop ideas and recommendations how to address them. In order to operationalise these tasks for each of the session topics a number of sub-questions were presented to the participants.

[1] See appendix

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

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?
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?

After an introduction at the opening session, briefly presenting the PANELFIT project and the specific objectives of this workshop, the three task-focused sessions followed a similar procedure and structure. After presenting the session topic and answering related questions, the participants were in an individual brainstorming phase asked to write down their ideas and responses on separate “sticky notes”, which were afterwards collected by the session moderator and notetakers. In a second phase the individual contributors were asked to briefly describe and explain their ideas to the workshop participants; this phase served to clarify possible misunderstandings and also to perform a first clustering by the session moderator of the brainstorming results on challenges, gaps and issues, as well as ways to fill them. In a subsequent phase the clustering was improved with the assistance of the participants, including the possibility to discuss and comment the results. Sessions 2 on gaps and issues and session 3 on ideas and recommendations how to fill or to solve them included also phases of prioritisation. In this phase the participants could indicate which issues and gaps they regarded as most important and which measures as most urgent to meet the challenges. Figure 1 illustrates the intermediate outcome of one of the workshop sessions.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039.

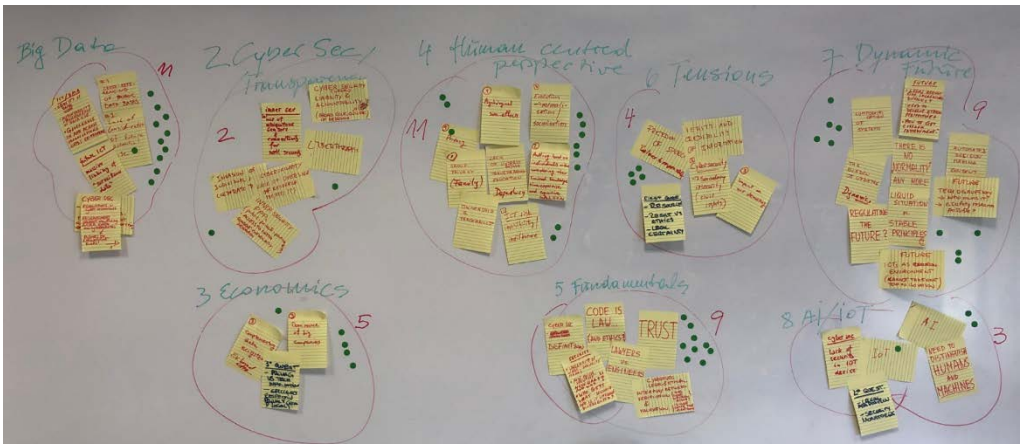

Figure 1: Preliminary clustering and prioritisation at the workshop

During clustering and prioritisation necessarily not all of the identified gaps and raised issues were taken fully into account. Nevertheless, the elaboration of the Issue & Gap Analysis by the PANELFIT partners involved in WP4 aimed at keeping the spirit of the workshop and addressing all of the main concerns raised and discussed during the workshop. Additional topics, which were identified at later stages, were also included if regarded as relevant for the addressees of the critical analysis.

The interim result of that effort was the elaboration of a preliminary draft of the "Issues and gap analysis on security and cybersecurity ELI in the context of ICT research and innovation". This draft was provided to twenty additional experts who attended a common workshop held in Madrid between 2nd and 4th March. All of them were given the chance to provide feedback on the document and valuable comments were gathered. On the basis of this feedback, a renewed version of the document was built during March and April 2020. This second version was then reviewed by two experts participating in the first round of the Extensive Public Consultation in mid-May. Their comments were used to improve that second version and build the actual version of this deliverable. The external experts provided also very valuable advice on how to make best use of the results in context of the general objectives of the PANELFIT project, which will careful be considered and taken into account for the final deliverables of PANELFIT.

In the context of PANELFIT in general, "gap" is defined as a missing regulation, while "issue" is related to a current regulation that needs further clarification or resolution of conflicts. In the context of this report on security and cybersecurity, in some cases – and based on the characteristic of the issue at stake – these terms are used in a wider sense. Some of the challenges and concerns identified and discussed at the expert workshop are related to matters beyond legislation, connected for instance to global political trends or economic relations. Accordingly, the anticipated risks and impacts for research and innovation or identified mitigation measures also address issues beyond ICT-related R&D, reflecting the need for more holistic approach of research activities to tackle urgent issues of security and cybersecurity. In this deliverable the term "privacy" is used in a broader understanding, substituting also legally

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

more exact terms like “respect for private life” or the “protection of personal data”, reflecting also the broad use that is made in literature and legislators.[2]

[2] For a more detailed discussion on the concepts of “privacy” see for instance: Porcedda, Maria Grazia (2017): The Recrudescence of ‘Security v. Privacy’after the 2015 Terrorist Attacks, and the Value of ‘Privacy Rights’ in the European Union. In: Rethinking Surveillance and Control. Nomos Verlagsgesellschaft mbH & Co. KG, S. 137-180.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2 Critical Analysis: Security and Cybersecurity

2.1 Definition of security and cybersecurity

2.1.1 Context

There is no universally agreed upon definition of security. Various disciplines tend to fill the term with strongly diverging meanings. Defining the context might help to clarify the meaning of the term in specific disciplines.[3] This can happen on various levels of abstraction. For example, information security may encompass the protection of concrete data sets while public security might be concerned with the much more abstract aim of safeguarding essential structures within a society. Important questions about context include what the protective aim is, against what threats it shall be secured and what protective measures shall be used.

2.1.2 Issue/gap

The lack of a consensual definition of security across various disciplines makes the term susceptible to reinterpretation based on implicit assumptions from various stakeholders. Requiring these assumptions to be stated explicitly fosters transparency and allows to challenge the otherwise opaque assumptions if required. Legal acts which allow derogations or restrictions to on the grounds of security may cause substantial legal uncertainty if the term security is not defined more clearly.

2.1.3 Risk assessment and impact for research and innovation

The ambiguity of the term security when used without additional qualifications runs the risk of keeping aim and beneficiaries of the measures unclear. This ambiguity may impede a discussion on which kind of security is necessary and whether the proposed measures are proportionate. For research and innovation, unclear requirements in research calls stemming from the generic and unspecific use of the term security may result in large discrepancies between the work sought and actually performed. This may lead to an inefficient use of funds or efforts of funding agencies or researchers. A qualification of the term may therefore lead to a clearer picture for researchers and funding agencies alike.

2.1.4 Mitigation measures

The following conceptualizations aims to provide a basic framework for a definition of the term security and important principles when applying it.

[3] Brooks, D. J., 2010, What is security: Definition through knowledge categorization, Security Journal 23(3), 225-239.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

2.1.4.1 Protective aim

When it comes to the definition of security, one of the first questions to ask is always security for what or for whom? Shall certain assets, specific people, small groups or whole societies be within the protective aim? The more concrete these aims can be defined, the easier it is afterwards to agree on a threat model and protective measures. For example, it is relatively straight forward to define what assets shall be protected in physical or information systems (cyber) security. In contrast, agreeing on protective aims for nation or social security is much more difficult since these concepts tend to be much broader and their interpretation is often shaped by political debates and personal values. Security in these contexts should therefore always include a clear definition, on a level as concrete as possible, which protective aims are pursued.

2.1.4.2 Risk model

Once the protective aim is established, the question arises which (external) threats it shall be protected against. Even for physical assets, it is often not feasible to protect against all possible threat scenarios. For example, protection against natural catastrophes like earthquakes or tsunamis is often not viable. For each threat, the likelihood of occurrence must also be assessed and related to the associated impact on the protective aim. This is usually multiplying the likelihood of a threat with its impact, producing a quantity called risk. In practice, the risk model can only protect against a limited subset of threats and should therefore discuss which threats it considers relevant and why.

2.1.4.3 Protective measures

In order to uphold the protective aims against the modelled threats, protective measures are often necessary. Within the context of a field specific security definition, these can often remain abstract while they should be described as concretely as possible for specific projects. In practice, these measures often constitute the core of the project and should therefore refer to a well-defined protective aim and threat model for their justification.

2.1.4.4 Principles

In addition to contextualized definitions of security for specific domains, certain principles shall always hold when justifying a measure on the basis of security in practise. These are described in the next sections.

2.1.4.5 Transparency

In cases where security measures actually or potentially interfere with human rights, e.g. in the case of surveillance involving personal data, the decision process of arriving at the protective measures and the reasons for their justification shall always be transparently communicated.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

This entails a written, publicly accessible documentation of the decision process and steps taken to ensure compliance.

2.1.4.6 Liability

Every provision is only as good as its enforcement. Therefore, a natural or legal person responsible for upholding the provisions shall be explicitly named. In case of a violation of the provisions, this person shall be held liable. Liability shall not only consist of an assessment of non-compliance but also contain sufficient remedies ensuring that compliance remains economically preferable to non-compliance.

2.1.4.7 Suitable, necessary and reasonable measure

These criteria's stem from the proportionality test applied by the European Court of Justice. It entails that a measure must be suitable to achieve the pursued aim and should provide evidence for its effectiveness. The measure must also be necessary; "necessary in a democratic society" in this context does not have the flexibility of such expressions as "useful", "reasonable", or "desirable" but implies the existence of a "pressing social need" for the interference in question.[4] Proportionality is also meaning that there are no ways less intrusive to the interest of others to achieve the same aim. And finally, the measure has to be reasonable, meaning that it duly considers and balances competing group interests.

As the definition of cybersecurity already encompasses many aspects of technical security in the ICT field, we suggest in the context of PANELFIT two additional concepts of security with particular emphasis on aspects of national security and fundamental right security respectively. To highlight the connection with the proposed conceptualization of security, the **protective aim** is written in red (bold), the threat model in blue (double underscore) and the protective measures in green (single underscore).

Fundamental rights security aims to **protect the fundamental rights of natural persons under the CFR**[5] from state or private actor encroachment by challenging, preventing and circumventing measures interfering with these rights.

National security aims to **protect the overall functioning of the social and legal system of a state** from coordinated attacks by organized groups using surveillance, detection and prevention of specific forms of unlawful activities.

[4] Council of Europe/European Court of Human Rights, 2019, Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence, Updated on 31 August 2019: Council of Europe. https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

[5] Charter of Fundamental Rights of the European Union, OJ C 326, p. 391–407.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.1.4.8 Cybersecurity

In the case of cybersecurity, a wide range of pre-existing definitions exists. They usually centre around the protection of networked systems against threats impeding their confidentiality, integrity or availability, although these concepts are not always explicitly mentioned. For example, cybersecurity is defined in the Regulation of the European agency for cybersecurity[6] (ENISA) as:

> *'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;*
>
> *'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons*[7]

As previously, the colour scheme is used to align the definitions with the proposed security conceptualization. In the definition damage and disrupt roughly corresponds to the concepts of integrity and availability, while confidentiality is lumped into the "otherwise adversely impact". The definition of cybersecurity of Public Safety Canada is narrower in scope and does not explicitly include affected persons within the protective aim:

> *The body of technologies, processes, practices and response and mitigation measures designed* ***to protect networks, computers, programs and data*** *from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.*[8]

Another approach is to build on intellectual property rights and characterise the threat model as "*occurrences that misalign de jure from de facto property rights*"[9] within cyberspace. While this promises to encompass many of the other concepts, it hinges on common understanding of property rights, which differ from country to country despite harmonization efforts.

To ensure a uniform understanding of cybersecurity, the usage of the ENISA definition may therefore by advisable, since it encompasses the system user's protection without relying on other legal concepts, which may be country specific.

---

[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[7] Art 2 Z 1 and 8 Regulation (EU) 2019/881.

[8] Public Safety Canada. 2010. Canada's Cyber Security Strategy. Ottawa: Public Safety Canada, Government of Canada. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx.

[9] Dan Craigen et al, Defining Cybersecurity, in Technology and Innovation Management Review, October 2014. https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. *This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.*

2.2 Security over privacy?

2.2.1 Context and legal background

The relation between public security and individual privacy has changed dramatically in the last decades. Progress in ICT offers ever-increasing possibilities of generating, collecting and processing of personal data, creating corresponding desires to make use of this new resource, which is often regarded as the "oil of the 21st century", to increase effectiveness and convenience, to be exploited for commercial reasons and to improve security. In particular, in the context of security the fundamental right of privacy appears to continue to lose ground for several reasons. First, technical possibilities to collect data (IoT) and to analyse them (AI) are still accelerating, eliminating more and more of the remaining islands of privacy. Future ICT will also limit or remove individual capabilities to escape privacy intrusive technologies. ICT embedded in artefacts or the environment, technologies used by nearby persons or your social contacts are collecting personal data, regardless whether you are an active user or not. AI systems will be needed to make meaningful use of the sheer amount of data generated by countless IoT devices. Second, security often serves as thought-terminating cliché when new surveillance technologies or more competences for law enforcement are at stake. Although criticised frequently and heavily, a presumed trade-off relation between security and privacy appears to dominate public debates and political decision-making. Losses in privacy are presented as a price to pay for increased inner security, usually without proof of evidence that such a relation prevails in the actual situation.

In addition, as a so-called wicked term, security can easily be redefined or reused in a different context and never be finally procured. Whereas metaphors of a trade-off relation or zero-sum game can easily be disproved at the endpoints – without privacy no security exists, hundred percent security can never be reached, regardless how deep privacy intrusions are – certainly, there are areas in which more surveillance can improve security. For instance, video surveillance in multi-storey car parks helps against rational crimes such as car thefts, but not against offences committed in the heat of the moment.

When policies based on specific and narrow exemptions, in which surveillance contributes to security, are becoming a guiding principle of technology development and implementation, several issues arise, which are addressed in different sections of this report. One temptation is to focus attention to security issues for which (surveillance) ICT solutions can be imagined. In this sense, technological progress can be seen as a factor reinforcing existing trends of securitisation. Securitisation[10] means the transformation of political issues of partners into security matters, allowing the use of extraordinary means or introducing limitations to normally inviolable human rights. Instead of focusing on potential root causes of insecurity due to crime and terrorism, e.g. inequality or lack of social security, strategies are preferred for which ICT

[10] Buzan, B., Wæver, O., Wæver, O. and De Wilde, J., 1998, Security: A new framework for analysis: Lynne Rienner Publishers.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

pretends to provide answers and for which therefore political action can easily be proved. The principle of proportionality is also easily overlooked when "technology fix" strategies dominate. The proportionality principle would require that in each case the least intrusive option should be chosen. In addition, a surveillance technology fix tends to follow a "the more, the better" thinking. Thus, neglecting on the one hand the possibility that more data may lead to more false positives, unnecessarily binding limited resources of law enforcement agencies, on the other hand implement intrusions into human rights without security gains or even with adverse security developments. The combination of both trends, a more open attitude to make use of surveillance technologies and dramatically increasing capabilities of such technologies, threatens the very essence and core of the human right of privacy.

While threats to privacy and the principles of data protection are not limited to the sphere of security and cybersecurity, the risk appears to be greater and the situation to be more complex in this context. First, security is in comparison to the provision of personal services or to commercial objectives much higher ranked in the value pyramid. Second, also the legal context is less clear and strict in this domain. Public security objectives form the basis of one of the exemptions from the strict regulations of the GDPR.[11] The contents and regulations of the EU police directive[12] are essentially unknown to non-experts, i.e. the majority of ICT researchers. In addition, security and law enforcement remain competences of the member states, therefore different national regulations further complicate the formulation of common (legally binding) guidelines.

2.2.2 Issue/gap

The complexity of the relation between privacy and security and the manifold impacts that the concrete forming of this relation has on the individual enjoyment and exercise of human rights and on shaping the democratic and societal development urgently requires broad debates and political dialogue. More participation is needed to decide into which directions our society should develop and to develop more concrete regulations to avoid changes and tendencies in the direction of illiberal and undemocratic societies.

Security over privacy attitudes raise issues related to exemptions from general and strict privacy protection. Whereas these exemptions do not necessarily create legal gaps by themselves, as the EU police directive on national legislations normally provide sufficient guidance to apply

[11] Art 2 (2) (d) GDPR.

[12] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

standard data protection processes,[13] such liberations create incentives of unproportionate extensions of surveillance powers of law enforcement or the development of respective technologies. The second aspect may also directly concern individual topics within security research calls of the European Commission, involving conflicts for the involved researchers as the requested technological capabilities to be developed may not be used in an ethically or legally compliant manner.[14] In addition, such exceptions constitute issues in general for involved researchers with proficiency in ICTs; the applicability of such exceptions is often open to interpretation and requires legal expertise or knowledge of case law.[15]

Similar considerations apply to the mandatory retention of personal data, which might be considered as relevant in the context of security. Mandatory data retention is obviously in conflict with constitutional or human rights related to privacy or the presumption of innocence. Accordingly, the EU data retention directive from 2006[16] was declared invalid by the Court of Justice of the European Union in April 2014 because it did not meet the principle of proportionality and should provide more safeguards regarding the protection of fundamental rights such as respect for private life and the protection of personal data.[17] Nevertheless similar data retention schemes are in place, e.g. Passenger name record (PNR)[18] rules. The possibility to scan data generated in past from various sources, in combination with intensions of unrestricted access to such data by law enforcement and the objective of mandatory retention of potentially security relevant data, remains an issue challenging fundamental rights. The currently negotiated EU ePrivacy Regulation is in this context criticised as containing backdoors to reintroduce blanket data retention, not in the form of a mandatory legal requirement but by offering a number of permissions to process electronic communications data to private companies.[19]

---

[13] Schlehahn, E., 2018, Die Methodik des Standard-Datenschutzmodells im Bereich der öffentlichen Sicherheit und Justiz, Datenschutz und Datensicherheit-DuD 42(1), 32-36.

[14] The Seventh Framework Programme project INDECT (https://cordis.europa.eu/project/id/218086) is a prominent example for such conflicts. It was one of the projects being accused of developing fundamental rights intrusive activities, causing critical reactions in the press and in the European Parliament (Vermeulen, M. und Bellanova, R., 2012, European Smart Surveillance: What's at Stake for Data Protection, Privacy and Non-Discrimination, Sec. & Hum. Rts. 23, 297.).

[15] Greer, S. C., 1997, The exceptions to Articles 8 to 11 of the European Convention on Human Rights, Vol. 88: Council of Europe.

[16] European Union, Directive 2006/24/EC on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks. http://data.europa.eu/eli/dir/2006/24/oj.

[17] https://ccdcoe.org/incyder-articles/eu-data-retention-directive-invalid/.

[18] https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en.

[19] https://digitalcourage.de/blog/2019/eprivacy-private-data-retention-through-the-back-door.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.2.3 Risk assessment and impact for research and innovation

There is in general a high risk that future ICTs, instead of contributing to societal and economic progress, lead to limitations of individual rights and to the erosion of democratic principles and civil liberties. Research and innovation, which is oriented towards a one-dimensional and simplifying understanding of security and cybersecurity, is at risk to develop technologies, which do not contribute to the intended aims but endanger the fundaments of liberal democracies.

2.2.4 Mitigation measures and costs

Mitigation measures include raising awareness that research and innovation in ICTs must strictly respect fundamental rights and comply with ethics, regardless whether justified security concerns appear also to warrant violations of long-established values and rights. Awareness raising must also embrace institutions responsible for the development and implementation of research programs in order to avoid that research calls include topics, which are apparently in contradiction to democratic principles and human rights. A specific measure could be the involvement of all relevant disciplines, including citizens and civil society, in the development, implementation and supervision of security/cyber security related ICT research. Direct costs would be moderate and easily outweighed by more effective and less intrusive ICTs.

2.3 Conflict between stable principles and “liquid” situations

2.3.1 Context and legal background

Before entering into context and legal background of the conflict between stable principles and “liquid” situations, the meaning of both terms (stable principles and liquid situations) should be explained. Stable principles, in relation to a comprehensive understanding of security as scrutinised in section 1 Definition of Security and Cybersecurity, refers to situations in which written or unwritten “laws” provide for a social, political or economic environment in which trust in the respect for such laws and rules can be expected in general. This does not imply that they are not violated at all, but that violations are not accepted and usually followed by some kind of sanctions. In this sense, stable principles provide security to all citizens, based on the certainty that breaches will normally have negative consequences for those conducting the violations.

In contrast, liquid situations refer to observations that many of these principles, which formed for a long period a stable skeleton of liberal and democratic societies and dominated international relations between democratic and nondemocratic nations, appear to disappear or at least to become largely irrelevant when important decisions are at stake. The so-called “new normal” describes situations that have not been considered as normal at all in the recent past decades. Openly discussed objectives to implement illiberal democracies, opinions of populist politicians to regard human rights as old-fashioned barriers to implement their political will, the upraise of fake news, cumulating in an equal treatment of facts and alternative facts, the

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

negligence of international treaties and their replacement by so-called deals, that can be broken or changed at any time, the disregard of international law and UN resolutions are only a few examples of liquid situations. These developments lead to increasing insecurities. They can also concern to regulations affecting the development or use of ICT in the area of security and cybersecurity. The rejection of the use of so-called Troyan horse software by the Austrian Constitutional Court (see next paragraph) illustrates this relation. Vice versa, liquid situations can also influence investment decisions into advanced infrastructures and increase related insecurities by mixing up security considerations related to digital sovereignty (national or European provision of required hardware and software), cyber security considerations (suspicion about presence of hidden backdoors in hardware) and economic considerations or trade war aspects.

Another form of liquid situation can be observed in an increasing trivialisation of creation or change of regulations in highly sensitive areas. One example relates to the adoption of a so-called security package in Austria in 2018, of which several legal provisions were repealed as unconstitutional by the Constitutional Court (VfGH). The repealed provisions concern the concealed recording and storage of data for the identification of vehicles and drivers by means of image-processing technical equipment, the processing of data from section control installations by the safety authorities, the covert monitoring of encrypted messages by installing a program on a computer system, and the authorisation to enter premises, search containers and overcome specific security measures for the purpose of installing this surveillance programme.[20] Another example, raising comparable concerns, is the Royal Decree-Law 14/2019 of 31 October set in force in Spain, which adopts urgent measures for reasons of public security in the areas of digital administration, public sector procurement and telecommunications. This legislation has been criticized from different sectors and NGOs. "This Royal Decree-Law modifies the regulation on the internet and electronic communications in order to grant the government greater powers to control these technologies in a range of vaguely defined situations. The Decree-Law defines an access to the network increasingly administered by the state, with no obligation for a judicial ruling to limit the access. This could pose a threat to human rights, particularly to that of freedom of expression."[21] Liquid situations refers in this context to the fact that regulations with far-reaching effects on fundamental rights are adopted without sufficient debate or even against better knowledge about unconstitutional provisions.

The problem of liquid situations does, however, also extend to safeguards against such uncertainties. International law, international and national legal systems are also being increasingly challenged by the political system and political actors. Attempts to limit the stability or power of the legal system can be observed in different forms, from debates about the relative role and power of the political versus the legal system, the abuse of constitutional

[20] Judgement of the Austrian Constitutional Court (only in German, 11.12.2019). https://www.vfgh.gv.at/medien/Kfz-Kennzeichenerfassung_und__Bundestrojaner__verfass.de.php

[21] https://edri.org/spain-new-law-threatens-internet-freedoms/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

regulations for the safeguarding of day-to-day legal matters, the provision of insufficient financial personal resources to the legal system, or the implementation of legal reforms with the aim to increase political influence, to name but a few possibilities.

2.3.2 Issue/gap

Security and privacy standards in regulations need to be followed by researches. Liquid situations threaten this demand in several aspects, going beyond the insufficient or ineffective enforcement of existing regulations. Liquid situations as defined above is threatening the long-term stability of such regulations and the provision of reliable principles to be followed.

2.3.3 Risk assessment and impact for research and innovation

A main risk caused by the liquid situations described above are losses in the efficiency of research and development of new ICT's. Unclear situations concerning the regulations and principles for technologies to be developed can delay the development, lead to technologies, which cannot be deployed in an ethically compliant manner or create technologies, the use of which may cause large negative side effects.

2.3.4 Mitigation measures and costs

Mitigation measures against general and worldwide political tendencies is probably beyond the scope of the PANELFIT project. Nevertheless, the guidance and guidelines developed within this project may help to limit the negative consequences of instable and liquid situations. One possibility would be to put more weight and reliance on ethics and human rights as a more stable long-term orientation of development in ICT. A concrete measure would be awareness raising and education in ethics of persons involved in R&D, but also of the general public as users, buyers and generally influenced individuals of security and cyber security technologies. On a general policy level, decision regarding ICT research should take into consideration the societal impacts that the technology could have. Policy makers should adopt actions to foster awareness regarding technology in general among the public. In that way, researchers, that are part of the public, could benefit from those policies and apply such knowledge in their research practice.

2.4 Surveillance effects on humans

2.4.1 Context

The increasing availability of ICTs and data, paired with the perceived rise of security threats, may lead to the justification of an ever-growing security apparatus. The impact of surveillance on humans is, however, not to be neglected. Indeed, researchers observed a chilling effect where people adapt their behaviour, in order to comply with a certain standard. This "self-censorship" can be seen as a reaction to the fear of actual punishment, but also to the fear of the "stigma of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

being labelled or tracked by state actors as non-conformists, deviants, or criminals, or the broader concern that information gathered about such activities may be leaked or disclosed publicly, leading to embarrassment or used for nefarious purposes by third-parties".[22] This chilling effect was reason for the German government to pass the Census Act,[23] an act defining the right to informational self-determination. This construct has subsequently found entrance to European Law under the paradigm of right to privacy, which is also the principle underpinning the General Data Protection Regulation.

The debate on impacts of surveillance on humans has regained momentum in relation to the discussion of surveillance capitalism[24]. According to Zuboff "Privacy is having the right to decide how you want to live, what you want to share, and what you choose to expose to the risks of transparency. In surveillance capitalism, those rights are taken from us without our knowledge, understanding, or consent, and used to create products designed to predict our behavior". These products are then sold into new markets that she calls "behavioral futures markets". At each stage, "our lives are further exposed to others without our consent." In losing decision rights, we lose privacy, as well as autonomy and self-determination. Such rights don't vanish, she points out. "We lose them to someone else".[25]

Nevertheless, in the aftermath of terrorist attacks in the last years, countries all over the world have tightened their security measures; one of the best examples being France which introduced new anti-terror laws after extending for six times the state of emergency, which was called after the terror attacks in November 2015.[26]

When weighing the two arguments against each other – national security and the infringed human values like autonomy or privacy – it needs to be considered, that the magnitude of surveillance data nowadays reaches a new degree of intrusiveness both in terms of quantity and quality. In quantity because the smartphone usually is an all-day-and-night companion and in quality because the type of information that can be obtained has changed drastically.[27] As the technological progress has made the collection of data not only easily executable but also affordable (ibid.), the risk of permanent surveillance has become particularly high. Furthermore, as Bruce Schneier depicts, the increased surveillance does not necessarily

---

[22] Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. Berkeley Technology Law Journal, 31(1), 117–182.

[23] BVerfGE 65, 1 in 1983

[24] Shoshana Zuboff (2019): The Age of Surveillance Capitalism – The Fight for a Human Future at the New Frontier of Power, PublicAffairs, New York.

[25] https://harvardmagazine.com/2017/01/the-watchers

[26] France approves tough new anti-terror laws. (2017, October 4). BBC News. Retrieved from https://www.bbc.com/news/world-europe-41493707.

[27] Bernal, P. (2016). Data gathering, surveillance and human rights: Recasting the debate. Journal of Cyber Policy, 1(2), 243–264. https://doi.org/10.1080/23738871.2016.1228990.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

improve the security.[28] He argues that terrorist attacks are so rare that they cannot be accurately predicted, while the attempt to doing so leads to an immense number of false alarms (which cost a lot of money and resources). Besides, the "new" surveillance automatically turns any individual into a potential suspect.

2.4.2 Gap

The argument of public security may be exploited to justify an ever-increasing surveillance, which might not be proportionate in comparison to the negative effects of surveillance on humans. No existing instrument reliably ensures that arguments invoking public security are not (ab)used to justify disproportionate surveillance measures.

2.4.3 Risk assessment & impact for research and innovation

The risks that this entails are manifold. For instance, the surveillance does not only affect individuals' privacy, but the chilling effect may also change society by threatening fundamental rights such as the freedom of speech, of assembly and association, or the prohibition of discrimination.[29]Furthermore, the increased surveillance may also facilitate the possibilities for blackmail, discrimination, and persuasion. This is particularly sensitive since a precise accuracy is not necessarily crucial for (particularly commercial) profilers. Hence, people are not only running the risk of being correctly classified into an unwanted category, but also of an inaccurate profiling per se (ibid.).

For researchers the surveillance issue is relevant since research runs the risk of (unintentionally) contributing to the surveillance by collecting personal data, either by an abuse of the research findings for unethical purposes or by an involuntary leakage of data to unauthorized parties. This risk is particularly high if technical and organizational measures taken to protect the personal data (e.g. the identity) are insufficient.

Furthermore, if data subjects get the feeling of being surveilled, they might start to distrust any form of data collection. This could result in 1) reluctance to participate in research studies and/or 2) a deliberate falsification of data in research studies.

2.4.4 Mitigation measures and costs

The line between protecting individuals by surveillance measures and harming them is very thin. Policy makers need to be aware of this and weigh whether the intended or taken measures have the desired effect and whether these justify possible negative effects.

---

[28] Schneier, B. (2016). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (1 edition). New York London: W. W. Norton & Company.

[29] Bernal, P. (2016). Data gathering, surveillance and human rights: Recasting the debate. Journal of Cyber Policy, 1(2), 243–264. https://doi.org/10.1080/23738871.2016.1228990

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

For researchers it is elementary to be aware of the sensitivity of the data they collect and what it can be used for. The introduction of reasonable technical and organizational measures to minimize the risk of a data leakages is essential. Consequently, what is needed are compulsory awareness trainings for researchers as well as the definition of a clear standard for technical and organizational measures for data protection in research and innovation.

2.5 The dominance of big US companies

2.5.1 Context and legal background

ICT research relies heavily on a wide variety of technological tools and software solutions that offer researchers many advantages in their daily work. In order to gather resources and knowledge from different fields all over the world, research is often conducted by a group of researchers rather than a single individual. To manage these research projects and to stay in line with the project plan, it is important to communicate, monitor tasks and exchange files in the most effective way. The internet has created the possibility to use tools and software solutions to tackle these challenges, many of which being used by research consortia. Nowadays, tools for communication and project management are widely applied. Data is stored and analysed in the cloud with big U.S. technology companies (Big Tech) like Amazon, Microsoft and Apple being the market leaders. Conferences and meetings are being organized and promoted through Facebook while general business communication and networking is being conducted using dedicated social networks such as LinkedIn, belonging to Microsoft. Google, as the largest search engine worldwide, owns Google Scholar, a popular search engine for academic work, next to a wide variety of work-related tools. Similarly, Microsoft and Apple offer different work-related tools, solutions for project management, as well as the most widely-used operating systems (OS) for smartphones and computers. While individuals and researchers use these solutions on a daily basis, they rarely contemplate on the importance, and ubiquity, of these tools, as well as on the business practices of these companies.[30]

Nemitz (2018) provides an explanation on the reasons of the dominance of a few technology companies and combines this with the fact that these companies are also the market leaders in AI research.[31] The dominance can be explained through the accumulation of power in four aspects. These companies possess huge amounts of capital, they control the infrastructure on public disclosure, the own an extensive collection of personal data, and they are the leaders in the development and integration of AI into existing and future reservices. These factors continue to strengthen their position of power in the market, increasing the dependency of researchers on their services.

[30] For more information see: Zuboff, S. (2015) 'Big other: Surveillance capitalism and the prospects of an information civilization', *Journal of Information Technology*. Nature Publishing Group, 30(1), pp. 75–89. doi: 10.1057/jit.2015.5.

[31]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Although the Big Techs solutions and tools yield great benefit for researchers by supporting them in various aspects of their work, the use of these tools also comes with certain risks. Researchers are increasingly dependent on a limited number of companies that provide them with tools. Through network and lock-in effects, the likelihood of using different services decreases while at the same time the market position of the Big Techs is further strengthened. Researchers and research consortia therefore put themselves and their research data in risk of cyberattacks, such as denial-of-service or man-in-the-middle attacks. Data that is stored at another party can be stolen or manipulated. Communication between consortia members might not be encrypted, malfunctions of technology solutions may endanger a whole research project. Additionally, European researchers might not be aware of the fact that their data is located in the U.S., where data privacy and security are regulated differently than in the EU. Even if the points mentioned above are known by the researchers, European alternatives are relatively unknown, not available or cannot compete with the Big Techs services.

2.5.2 Issue

Big U.S. companies dominate not only technology development in general but also in the context of ICT research in particular. “Big Tech” meaning the major U.S. technology companies like Microsoft, Google, Facebook and Apple, are market leaders in the provision of software and technological tools used for and in research projects such as collaboration, project management and communication tools as well as data and cloud storage solutions and the subsequent tools for data analysis.

Furthermore, these big tech companies not only dominate these markets but they also dominate research itself in the field of Artificial Intelligence (AI). This might lead to a dominance in AI products in the future, whose implications have been discussed in the section *AI and Security* of this document, and an increase in dominance in the aforementioned technologies. Data, which these companies own, store and produce in great quantities is a competitive advantage in the development of AI.[32]

2.5.3 Relevance & impact for research and innovation

The dominance of U.S. companies in areas that affect European researchers can be considered problematic as it increases the dependence of European research on non-European tools and technological solutions. This in turn increases the dominance of the American companies, discouraging European innovation and weakening European competing organizations. For researchers, this dependency can be seen as a business risk as their work relies on these tools, either indirectly, in the case of project management or communication tools, or directly, if data

[32] Westerheide, F. (2019) *The Artificial Intelligence Industry and Global Challenges*. Available at: https://www.forbes.com/sites/cognitiveworld/2019/11/27/the-artificial-intelligence-industry-and-global-challenges/#53495c83deb9.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039.

is stored and analysed with the use of Big Techs solutions. If these tools become unavailable or unusable, either due to governmental regulation, extreme price increases or the failure of the solution itself, researchers are incapable of performing their work. This could lead to the failure of research projects if these risks have not been considered in the past.

Apart from that, data security and privacy issues need to be discussed. The regulation and requirements for cybersecurity within the U.S. differ greatly from the ones in the EU. This means on the one hand that the same level of protection is not guaranteed, while on the other hand, the prosecution of illegal activities is most likely to turn out difficult. This gains relevance as many researchers who are using these services are simply not aware of their data exiting the European Union and the legal consequences related to it. Failure of data and privacy protection leads to a loss of reputation for the researching party, which in turn leads to a direct decline in revenue or projects in the future. Additionally, the General Data Protection Regulation (GDPR) of the EU consists of strict and severe penalties for failing to ensure and protect data and information.

The dependence on and dominance of big U.S. technology therefore poses a threat to research and innovation in ICT.

2.5.4 Mitigation measures and costs

There exist several strategies to mitigate this issue, which will be discussed in the following. The strategies can be divided into strategies that support researchers in avoiding big U.S. tech companies and empowering them to use different, or personal solutions; and strategies that aim to either regulate, or break up, these companies. Naturally, different stakeholders may follow different strategies.

The first type of solutions focuses not on the dominant market players but on the researchers and European companies that provide tools and services for these researchers. Firstly, on an awareness level, it is advisable to educate researchers about the (legal) consequences that might follow by using services and tools from Big Tech companies. The goal would be to increase awareness on the dominance of these companies and the level of dependence of research in the EU on non-EU companies. As was discussed before, not only do researchers rely on them when working with every-day tools, but they also store their research, their data on servers from Big Tech. Additionally, communication between researchers among each other's, as well as with the general public takes place using platforms and services of Big Tech. This dependency poses a threat to the security and privacy of the researcher and their research objects.

After becoming aware of the problem at hand, researchers should be enabled find and use substitute solutions. Hereby, the use of already existing services provided by European entities should be supported and promoted, for instance by recommending them to project consortia. The EU, as well as the European countries themselves, could foster the creation and improvement of technological tools and solutions in order to create competitors that can match existing solutions by big U.S. companies. On the other hand, some of the services and tools used by researchers could be substituted by own solutions e.g. an own data repository for data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

storage and distribution, instead of a bought service. Basic trainings should be offered to provide the necessary technical knowledge and skills to set up and design fitting solutions. This offer could be underpinned by a support line for possible questions, as well as a repository of existing, open source solutions. Lastly, as a long-term solution the provision of a project management platform run by the European Union itself would be preferable, in order to ensure independent and secure research projects. The project "GAIA-X" by the Federal Ministry for Economic Affairs and Energy (BMWi) of Germany can be seen as an example of such an endeavour. The project, based on EU-principles of data privacy and security, aims to create a connected infrastructure for data sharing and collaboration in the EU.[33] Another example is eduMEET[34], a video conferencing platform developed by an EU funded project.

On a global scale, the EU is already aiming to regulate Big Tech in order to combat monopolies or to hinder them on becoming even more powerful. Several strategies can be followed that are not aiming to break up monopolies and companies but instead level the playing field for new entrants.[35] Breaking up companies is hard to legally enforce, especially if the companies are headquartered in non-EU countries. Instead, a first step might be mandatory data sharing for Big Tech. The advantage of this solution is that consumers are not affected. While breaking up a company, provided the execution is legal in the first place, can have drawbacks for users, as the services of these companies might get worse, mandatory data sharing is not affecting users or consumers. Instead, smaller companies gain access to anonymized data that Big Techs own, enabling new entrants to compete with larger players.

A second option would be to prohibit Big Techs from favouring their services on their own platforms. The Big Techs provide platform business models on which they know increasingly provide services on one side of their own platform. An example can be given with Google, which produces the operating system (OS) Android for smartphones. Smartphone users are now able to download and install applications on their smartphone. Additional services that are being requested might also come from Google, such as Google Drive or Google Docs, that are also being used in research collaboration and data storage. The tools and services from Google are now competing against similar tools from other companies. However, Google, as the platform provider is now able to discriminate their own solutions in favour of those from other companies. Non-discrimination policies would be able to prevent this, giving Big Tech the opportunity to compete with other companies on their own platform, without artificial

[33] Federal Ministry for Economic Affairs and Energy (BMWi). (2019) *Project GAIA-X*. Available at: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=16

[34] https://edumeet.org/

[35] Chen, A. (2019) 'How to regulate Big Tech without breaking it up', *Technologyreview*. Available at: https://www.technologyreview.com/s/613640/big-tech-monopoly-breakup-amazon-apple-facebook-google-regulation-policy/.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

advantages. The EU has already found Microsoft guilty of similar charges in 2004[36] and only recently Google in 2017[37].

Another solution to foster competition would be the introduction of data portability and data interoperability. These concepts weaken the lock-in effect and network effect of the business models of Big Tech. Data portability hereby ensures that users can move their data and information from one company or platform to another one. Large companies themselves are already providing solutions for data portability themselves, as can be seen in the example of Apple and other Smartphone manufacturers. In order to enable buyers to switch from one manufacturer and OS system to their own, companies created technical solutions to enable the transfer of data and information from one smartphone to another. Similar solutions could be made a requirement for communication or collaboration tools too. Analogously, data interoperability is used to describe the ability of different services to work together along different platforms. Again, data interoperability has been enforced in the past, as seen in the case of the merger of Time Warner and AOL in 2001. [38]

Lastly, an additional solution would be to restrict companies in their business models or to restrict their data collecting behaviour. Germany's competition authority for instance prohibited Facebook to combine and gather data on users from non-Facebook websites and to combine this data with information from their site. [39] Through this action, users are given the choice to opt-in for data collection, while Facebooks market power is weakened without breaking up the company.

All the solutions mentioned beforehand aim to weaken the dominance of Big Tech without tackling the underlying problem directly. As monopolists, or platform providers that compete on their own platform, the market dominance in software business could be broken by breaking up the monopolists. While a public debate on this topic is currently happening in the U.S., with Senator Warren, a presidential contender for the 2020 election, as well as President Trump, both voicing possibilities in this direction, the question if this is legal has not been answered yet definitively. [40] It is not clear if Big Tech companies have actually violated antitrust laws.

---

[36] Official Journal of the European Commission. (2004) *Commission Decision* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0053&from=EN

[37] Official Journal of the European Commission. (2017) *Commission Decision* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018XC0112(01)&from=EN

[38] See CNN.Money. (2001) 'AOL Time Warner gets OK' Available at: https://money.cnn.com/2001/01/11/deals/hold_aol/.

[39] Singer, N. (2019) *Germany Restricts Facebook's Data Gathering.* Available at: https://www.nytimes.com/2019/02/07/technology/germany-facebook-data.html

[40] Rainey, T. (2019) *Breaking-Up Big Tech.* Available at: http://www.bu.edu/articles/2019/break-up-big-tech/.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

While European countries and the EU are quicker on regulating markets, the U.S. follows a more laid-back approach with a less regulated free market.

2.6 Information and power asymmetries

2.6.1 Context/background

"Knowledge is power." (Francis Bacon)[41]

Bacon originally wrote about the power of science: generating knowledge based on scientific methods. Later on, this quote was used amongst others by proponents of the labour movement to demand access to knowledge for common people and thereby redistribute the power more equally within society.

Power, in all its dimensions, was also one of the central themes of Foucault's work. In his book Surveiller et punir (1975, English title: Discipline and Punish: The Birth of the Prison) he wrote about the nature of power coming from surveillance and the knowledge thereby gained. Surveillance constitutes a power asymmetry by giving knowledge/power to the party surveilling and leaving the surveilled ones in a position of relative weakness.

In today's digital era, people are becoming kind of data leaks themselves: by constantly producing and (involuntarily) sharing data about their (digital) lives. Several organisations and other parties are interested in these data – in collecting, storing, analysing and monetising them. As a result, people are constantly watched by these organisations and parties, creating the data for them, just to be in a permanently inferior position, and sometimes even dependant on their surveillant e.g. from state or government services or from private insurance companies.

2.6.2 Issue/gap

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.

As an example, private companies can define sets of rules for automated decisions by algorithms that do not comply with national laws, but rather enforce their way of thinking and the values of the algorithm's programmers and/or the company's owners and shareholders.

The concentration of financial power and the inconceivable amount of data collected by big platform companies (like Google, Amazon, Facebook, Alibaba etc.) give them a corresponding

[41] Originally Bacon wrote in Meditationes Sacrae (1597) „Nam et ipsa scientia potestas est." One year later, he translated this into English: "(For) Knowledge (itself) is power".

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

advantage in an unregulated market, further increasing their power. Due to network effects, they are more attractive for the more users they have, so they grow bigger still and marginalise or take over smaller competitors. On the basis of the collected data, they are then able to develop better algorithms and new ways of making money from data, and in much faster ways than others. This again gives them a further competitive advantage on the market. This commercialisation of data gained by surveillance measures is named 'surveillance capitalism'[42], and is currently a very successful business model, also because of the lack of effective enforcement of laws and regulations in the field of data protection.

A further problem related to the given setting of asymmetric power is (industrial) espionage, which is easier if the data are already transferred to countries which might be interested in the data or in which 'security' legislation allows access to law enforcement or intelligence services. This issue is closely related to the question of individual autonomy and digital sovereignty: how much control do individuals or states have if they are not controlling their data?

2.6.3 Risk assessment and the impact for research and innovation

Whoever owns and controls the data, is able to tell where it comes from, and whether it has been altered or manipulated, and to decide whether to alter the data themselves. Hence, data ownership brings great responsibility – but can we trust in big, commercial companies, to handle and protect our data in a responsible and effective way? Governments, agencies or other actors can put pressure on these companies to share or alter the data, and restrict access to it or access to certain services. The question, though, is of dependency versus autonomy, once we have handed over all our data. This has become a question of sovereignty for individuals as well as states and democracies: how can we to control what happens to relevant information and data?

In the R&I field in particular, the matters around cybersecurity and industrial espionage are extremely important. It is difficult for many SMEs to maintain the skills to counter cyberattacks or protect their assets, and virtually utterly impossible for individual consumers on their own to stand up against big companies or foreign political interests by themselves. Therefore, it is of utmost importance to give data only to trustworthy entities, and, even then make sure it is protected on a technical level (e.g. through encryption) as well.

The so-called 'chilling effect' – where people, because they feel under surveillance, start to conform and behave in the way they think others expect them to is always a risk when exercising surveillance pressure on society. As a result, that non-conformist behaviour, dissenting opinions and in general ways of living which encourages discourse, innovation and evolution in a society, are all suppressed.

[42] Shoshana Zuboff (2019): The Age of Surveillance Capitalism – The Fight for a Human Future at the New Frontier of Power, PublicAffairs, New York.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.6.4 Mitigation measures

It is clear that the practices of ignoring data protection regulation, adopted by some companies and states, must end. Therefore, all relevant actors, and especially the national DPAs, must be supported in their efforts to enforce data protection laws and assert citizens' rights. In this way, citizens will become more independent, more aware and could possibly be freed from the inferior power position of surveilled subjects.

If companies provide basic services to society that everyone should be able to use (which services qualify for this status is a political decision), they must operate under a strict regime, as telephone companies did in the past, for example. In exchange, companies could be supported by the government when they have to provide a service in areas where they are not able to generate profit.

Furthermore, people should be able to choose which company delivers the best service for their needs. Therefore monopolies (or cartels) should be avoided, as well as proprietary systems, lock-ins and data which cannot be moved to other providers.

More transparent and clearly phrased data protection agreements between companies and their customers, or even standardized clauses or icons as suggested in the GDPR (Art. 12(7)), could also help to in distribute power more equally between companies and citizens. The many very vague agreements that exist today often leave customers in the dark about the kind of personal data used by companies, the purpose(s) for which it is used, and who else receives their data.

To deal with big platforms and network effects, strengthening innovative SMEs, local alternatives and consumer protection agencies would likely tip the power balance between consumers and providers towards the former, setting a fairer scene in which the contractors meet on an equal footing. Other effects of having all the big platform companies in the USA[43], such as financial dependency and the 'knowledge drain' etc., could be countered by setting up a business environment and a regulatory framework that fosters the formation of a European data ecosystem that goes beyond GAFA[44] and supports data portability.

In this regard, it is useful to think of publicly available sets of training data for algorithms. These could be used to train the systems, or to certify against them. This would improve the situations of small companies that cannot count on vast amounts of in-house available customer data.

To share the control of the internet equally, it will be necessary to negotiate fair governance principles amongst ICANN, RIPE and all the other regional internet registries. This could help to avoid situations where governments for political reasons would try to instrumentalize the non-profit organisations that control the internet infrastructure.

[43] Those in China are not used in Europe on a significant basis.

[44] The four big companies that influence the digital economy and control much of the data-generated revenue are: Google, Apple, Facebook and Amazon, often referred to as 'GAFA'.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

Under certain conditions, it is useful to share, sell, lend or otherwise use data in a commercial way. However, the rules under which this can be done should be a political decision, that is informed by experts and a public discussion. The rules should be as clear as possible and they should be set in advance, if politicians want to decide before companies and the market do so. By creating a fairer scene for data commercialisation, governments and administrations will also better be able to control and /monitor data trading to make sure it adheres to the ethical standards that citizens wish to be followed.

2.7 Future impacts on democracy

2.7.1 Context and legal background

The opportunity to live in a democratic society is a decisive factor in the security of citizens. Respect for democratic principles and of the rule of law provides basic protections against the abuse of state powers and political arbitrariness. Accordingly, in most liberal states, democratic norms and principles are anchored in the constitution.

There were widespread expectations and hopes that progress in ICTs would bring positive impacts on democracy. These were predominantly linked to the first waves of digitalisation and the advent of the internet: it was presumed that the growth and spread of ICTs would lead to better informed citizens, reduce barriers to participation in democratic deliberation and decision-making, and thus foster and spread out democratic traditions in significant ways. These expectations of citizen empowerment were not met, however, and have given way to a much more realistic and sceptical assessment of the impacts of current and future ICT on democracy. The observed erosion of democratic principles in many countries, for example through the rise of governments and political leaders, who obviously violate democratic rules and openly declare their disregard of such rules and of human rights, is often directly or indirectly linked to misuses of ICT applications or services. A prominent discussion in this context concerns the influence that cyber-attacks, botnets and unlawful harvesting of social network data have had on the results of the presidential elections in the United States.

The still ongoing digital revolution has the power to change how societies at large function, and how individuals live, in a great so many ways. This raises a number of concerns about the survival of democracy, though[45]. ICTs can be used to inform as well as to misinform. Well-known examples include (successful) attempts to influence democratic elections through the massive and targeted distribution of (fake) news via social networks[46].

---

[45] Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., van den Hoven, J., Zicari, R. V. and Zwitter, A., 2017, Will democracy survive big data and artificial intelligence, Scientific American 25 https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/.

[46] Gurumurthy, A. and Bharthur, D., 2018, Democracy and the algorithmic turn, SUR-Int'l J. on Hum Rts. 27, 39 https://sur.conectas.org/en/democracy-and-the-algorithmic-turn/.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Threats to democracy are, however, not restricted to the manipulation of voters or of individual elections. Owen[47] regards "… the way data is collected and monetized (surveillance capitalism), and how our reality is algorithmically determined through artificial intelligence (AI)" as the main structural problems enabling misinformation." The current unprecedented accumulation of economic power among a few internet giants is being accompanied by a concentration of control of digital infrastructures, of capabilities to collect and process personal data, and a resulting domination in the development of AI systems[48].

Such assessments indicate more fundamental and structural concerns for the future of democracy. Economic power transforms into political power, either directly or in less direct ways (e.g. through lobbying activities). De facto monopolies, with regard to access to big data and the use of this resource, allow to create superior AI technologies and services; naturally, this also creates incentives to abuse this capability to expand and secure economic and political power in the future. Apart from the general incompatibility of monopolies with free societies and efficient markets, additional concerns in the context of the European Union are linked to the fact that all dominant players in this domain are currently US-based. ICTs also plays also an important role in safeguarding the continued existence of undemocratic systems, with China's 'Citizen Scores' system[49] being a prominent example for such tendencies.

2.7.2 Issue/gap

It is fair to say that our 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 and immediate interventions to stop and reverse the antidemocratic impacts of existing and future ICTs. Many details of the activities needed remain unclear, though, and there are several questions that need answering:

- Are existing regulations (e.g. the GDPR), effective and sufficient in mitigating the numerous concerns? Which?
- Which additional measures are needed, and at which levels?
- Who should be involved in their development, and who should be responsible for their implementation and enforcement?

[47] Owen, T. (2018). Ungoverned space: how surveillance capitalism and AI undermine democracy. Centre for International Governance Innovation, March, 20. Retrieved from https://www.cigionline.org/articles/ungoverned-space

[48] Nemitz, P., 2018, Constitutional democracy and technology in the age of artificial intelligence, Philos Trans A Math Phys Eng Sci 376(2133) https://www.ncbi.nlm.nih.gov/pubmed/30323003.

[49] Botsman, R., 2017, Big data meets Big Brother as China moves to rate its citizens, *Wired UK 21*.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

- Do existing manifestos and sets of principles, such as for instance the Vienna Manifesto on Digital Humanism[50], provide coherent and implementable advice to guide the future development of ICTs?
- In what ways can the numerous initiatives[51] to provide specific guidance for the development and use of AI be applied in the context of security and cybersecurity?

2.7.3 Risk assessment and impact for research and innovation

The sheer magnitude of the risks to democracy, and their multiple dimensions, create on the general level the risk of focusing on individual aspect(s), with the consequence that individual measures developed may turn out having little or insufficient impact on safeguarding of democratic principles in the future. Research and innovation should therefore consider the complexity of the economic, political, social and technical developments and tendencies responsible for the deterioration of democratic traditions. The assessment of ICT's should therefore also analyse the specific role(s) that technology plays in these developments, e.g. for example as initiator and driver, as enabler and enforcer, or and as a tool being misused to pursue certain interests.

2.7.4 Mitigation measures and costs

The complexity and multidimensionality of the involved issues, as well as the fact that the very core of living in liberal societies is threatened, demand for a corresponding approach in developing mitigation measures. Interdisciplinary research that involves all relevant stakeholders and actors, including civil society organisations and citizens as (representatives of) concerned individuals is needed. Depending on the kind of measures developed and regarded as appropriate, the costs could be assessed on a scale from between moderate (e.g. implementation of effective regulations, education and awareness raising, etc. cetera) to extremely high, in monetary terms and in terms of political resistance (e.g. the break-up of monopolies or the establishment of European infrastructures that compete with existing US-based ones).

[50] Werthner, H., Lee, E. A., Akkermans, H., Vardi, M., Ghezzi, C., Magnenat-Thalmann, N., Nowotny, H., Hardman, L., Stock, O., Larus, J., Aiello, M., Nardelli, E., Stampfer, M., Frauenberger, C., Ortiz, M., Reichl, P., Schiaffonati, V., Tsigkanos, C., Aspray, W., Bruijn, M. E. d., Strassnig, M., Neidhardt, J., Forgo, N., Hauswirth, M., Parker, G. G., Sertkan, M., Stanger, A., Knees, P., Tamburrini, G., Tellioglu, H., Ricci, F. and Nalis-Neuner, I., 2019, Vienna Manifesto on Digital Humanism, Vienna https://www.informatik.tuwien.ac.at/dighum/ .

[51] See https://ai-hr.cyber.harvard.edu/primp-viz.html for a comprehensive summary of AI principles.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.8 Freedom of expression

2.8.1 Context

Freedom of expression is a central building block of democracy if one understands democracy inter alia as a form of government that offers as many people as possible the opportunity to participate in the public discourse. However, this presupposes that all members of society, especially members of minorities and those with differing opinions, are able to express their views freely and without fear of repression. The freedom of expression guarantees that everyone has the opportunity to speak freely and without fear, to express attitudes, criticism, fears or ideals. Furthermore, it is equally important to hold public authorities accountable.[52]

The legal bases for this freedom are laid down in Art. 19 of the Declaration of Human Rights[53], the Art. 10 of the European Convention on Human Rights,[54] in the Art. 11 of the EU Charta of Fundamental Rights[55] and in Art. 19 of the International Covenant on Civil and Political Rights. [56] These articles not only state that everyone has the right to freedom of expression and opinion; in order to be able to exercise that right it is also fundamentally important to have access to information, without interference from public authorities and regardless of frontiers.

The freedom of expression is, on the one hand, a specification of the underlying more abstract ideas of autonomy and freedom and, on the other hand, the basis of other important fundamental rights and freedoms like the one of the arts and sciences (Art. 13 EU Charter of Fundamental Rights).[57]

As other fundamental rights, the freedom of expression is not unlimited. Paragraph 2 of Art. 10 of the European Convention on Human Rights states that this right also bears obligations and might lawfully be restricted within narrow boundaries if necessary. In democratic societies potential lawful bases are in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.[58]

---

[52] Mendel, T., 2017, A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights, 21/02/2017: Council of Europe. Centre for Law and Democracy http://rm.coe.int/09000016806f5bb3

[53] https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf or https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

[54] https://www.echr.coe.int/Documents/Convention_ENG.pdf

[55] https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[56] https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

[57] https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[58] https://www.echr.coe.int/Documents/Convention_ENG.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

Furthermore Art. 17 of the Convention on Human Rights states that no provision of the Human Rights Convention may be construed as leading to the abolition of the rights and freedoms set forth therein.[59] Democracy and human rights must not be undermined and destroyed on the grounds of freedom of expression.[60]

According to paragraph 2 of Art. 11 of the EU Charter of Fundamental Rights the right to information entails the freedom and pluralism of the media. It underlines the importance of a free press for democratic systems. Access to pluralistic sources of information is a prerequisite for transparency of democratic decision making. Transparency in turn is key when it comes to control those in power and safeguard democracy. Therefore, the protection of whistle blowers and editorial secrecy are also particularly important. Those who have the courage to pass on information should not, however, be forced to go public themselves. They should not be forced to endanger their profession, their existence or their friends and family by having to go public themselves.[61]

2.8.2 Issue/gap

Social media provide an almost infinite number of possibilities of expression for citizens. On the one hand, this could lead to a stronger democratisation of the public discourse, but it also, leads to the emergence of "hate speech" and disparagement under the "protective mantle" of freedom of expression.

As stated above the right to information entails the freedom and pluralism of the media. Pluralism is inscribed in the social media, since theoretically anyone can and is allowed to publish. However, the use of algorithms in a manipulative way in social media (e.g. when using micro-targeting to influence people's social or political behaviour) may limit people's access to a variety of information, fostering so-called filter-bubbles and this (in certain cases) may pose a real threat to our democracies.

Furthermore, social media can be used to communicate and organise groups with a wide variety of objectives. With regard to inner security, more attention is being paid to this aspect. There are repeated attempts to restrict freedom of expression with reference to anti-terrorist measures and inner security. Besides mass surveillance of social media and internet usage, measures to this end include the obligation to register and to use clear names when using social media. The restriction of anonymity or of the use of pseudonyms, however, may lead in return to the restriction of societal discourse and thus restricts freedom of expression.

---

[59] A similar statement is made in Art 53 Charter of Fundamental Rights and in Art 53 ECHR, which are both directly applicable law within the European Union.

[60] Mendel, T., 2017, A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights, 21/02/2017: Council of Europe. Centre for Law and Democracy http://rm.coe.int/09000016806f5bb3

[61] https://www.unsereverfassung.at/wp-content/uploads/2017/02/Meinungsfreiheit_unsereVerfassung_2017.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

In many cases, measures against fake news or hate speech can be a matter of ensuring the authenticity and trustworthiness of information (fact checking) or preventing the dissemination of unwelcome or dangerous information. The main question remains: how far can democratic societies go and which institutions should be responsible? This also refers to the ongoing discussion on the needed level of judicial control of law-enforcement measures.

Democracy thrives on criticism and discussion. To achieve this, we often need a level playing field that opens the opportunities for minorities and those not in power, to be able to create attention. In a democracy, it must be possible to criticise and even challenge authorities, companies, religious communities and influential persons without fear of persecution. Under certain circumstances this can be offensive or insulting for (many) people. Often it is not easy to determine when this "red line" is crossed. It depends a lot on the context and personal attitudes, views and cultural habits. The European Court of Human Rights is therefore increasingly emphasising journalistic due diligence when it comes to freedom of expression. Calls for violence and hatred, articles and contributions that question the democratic constitution and human rights cannot be justified by media freedom.[62]

Most communication nowadays takes place in the Internet on privately owned and controlled platforms. It is largely unclear how these platforms are monitored, how the governing algorithms work and whose values are ruling. Because of the magnitude of users on these platforms, they play an important societal role, but are not legitimized in a democratic way. This leads to problematic situations of potential private hyper-censorship at the hands of social media giants?[63] Do we therefore need to demand that the policing of free speech ends and that corporations are not turned into the surrogate for a police state none of us voted for?[64] Platforms like Facebook and Twitter have immense power over public discourse. When they decide content is not fit for public consumption, it can disappear forever, like in a black hole.[65]

Concluding, we may see the freedom of expression is endangered by rampant hate speech, trolling, bullying and inappropriate use on the one side, which on the other triggers stricter public and private surveillance, content control and private censorship. This again may lead to a so-called chilling effect, which means self-censorship and anticipatory obedience.

2.8.3 Risk assessment and impact for research and innovation

The freedom of arts and sciences is a directly related to the freedom of expression. In research and innovation contexts, both freedoms must therefore be given special consideration. The freedom of science means freedom of thought, but also the freedom to share thoughts with others, by publishing them. This freedom is affected on the one hand by high publication fees

[62] https://www.unsereverfassung.at/wp-content/uploads/2017/02/Meinungsfreiheit_unsereVerfassung_2017.pdf

[63] https://www.forbes.com/sites/julianvigo/2018/11/28/big-techs-threat-to-freedom-of-expression/

[64] https://www.forbes.com/sites/julianvigo/2018/11/28/big-techs-threat-to-freedom-of-expression/

[65] https://www.theguardian.com/commentisfree/2018/sep/06/facebook-twitter-free-speech-sandberg-dorsey

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

of private publishers, but also by confidentiality clauses and other restrictions in certain research contexts. Particularly in publicly funded research, it seems necessary to help the approaches of Open Access and Open Science to achieve a breakthrough. In special research areas, such as cybersecurity, military or dual-use research, there may be restrictions on freedom of opinion and research. Here, public funding in particular must ensure that these restrictions are either not implemented at all or only to an adequate extent.

2.8.4 Mitigation measures

With the fundamental right to freedom of expression and freedom of science and research, there is a strong set of rules whose observance is monitored by the European Court of Human Rights and the European Court of Justice. However, to ensure that the above-mentioned rights are not impaired, measures to raise awareness, but above all a high degree of transparency in funded research, Open Access publications and good networking among researchers should be achieved.

In early 2019, the European Court of Human Rights reiterated its standing jurisprudence that the effective exercise of the freedom of expression is not dependent merely on the state's duty not to interfere, but may call for positive measures of protection. "In particular, the positive obligations under Article 10 of the Convention require states to create, while establishing an effective system of protection of journalists, a favourable environment for participation in public debate by all the persons concerned, enabling them to express their opinions and ideas without fear, even if they run counter to those defended by the official authorities or by a significant part of public opinion, or even irritating or shocking to the latter".[66]

2.9 Biometrics and ICT for emotion detection

2.9.1 Context

In recent years technological developments have led to biometrical analysis becoming economically more and more feasible for mass use.[67] The ubiquitous usage of digital devices equipped with cameras and microphones results in biometric audio-visual information being readily recordable in many circumstances. The possibility of using biometric technologies to

[66] Khadija Ismayilova v. Azerbaijan, 65286/13 and 57270/15, 10 January 2019, in: CoE (2019) Freedom of Expression in 2018, https://rm.coe.int/freedom-of-expression-2018-/1680943557

[67] Art 29 Group, WP193 Opinion 3/2012 on developments in biometric technologies, p. 16

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

analyse facial movements and mimics or speech patterns has created strong interests to harvest this information for emotion detection.[68]

Such an analysis of biometric data is considered processing of special categories of personal data under the EU General Data Protection Regulation (GDPR) and therefore only allowed if the conditions of a certain legal basis are met.[69] Among those are the explicit consent of the data subject for the specified purpose or processing necessary for scientific research purposes or statistical purposes.[70] For scientific research or statistical purposes, the GDPR allows member states to create a legal basis based on national legislation which has to "respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject".[71] This opening clause might, however, lead to large differences for research conditions in member states with regards to data processing.

Furthermore, it remains unclear whether facial expressions or speech patterns are reliable and accurate indicators for emotion status. A recent survey studying the use of facial expression for emotion detection found that there is no simple one-to-one correspondence between facial expression and prototypical emotions.[72] Similarly, assessment of the emotions conveyed by speech patterns can vary widely depending on perception the particular (human) evaluator.[73] Despite the inherent uncertainty associated with such judgements, for the people affected by such systems a subjective assessment may therefore be mistaken for an objective truth. While additional context (i.e. combination of speech and facial movements) might improve the emotion detection, the issue remains that people are affected by the systems assessment, irrespective whether it is accurate or not.

2.9.2 Issue/gap

One of the main issues with biometric analysis based on audio-visual data is that it is often opaque for data subjects whether such an analysis is performed.[74] This may as a consequence

[68] Ghosh S. et al., Towards designing an intelligent experience sampling method for emotion detection. In: 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2017. p. 401-406.

[69] Art 9(2) GDPR

[70] Art 9(2) (a) and (j) GDPR

[71] See Art 89 (2) GDPR for general scientific research purposes and in addition Art 9 (2) (j) GDPR for special categories of personal data

[72] Feldman Barrett L. et al, Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, *In:* Psychological Science in the Public Interest, 20(1), 2019

[73] Schuller B., Speech Emotion Recognition - Two Decades in a Nutshell, Benchmarks and Ongoing Trends, *In:* Communications of the ACM, 61(5), 2018, p. 98

[74] Kindt E., Privacy and Data Protection Issues of Biometric Applications, Springer, 2016, p. 350 paragraph 119

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

lead to discriminatory treatment based on the analysis results and enable covert identification. Affected persons may not even be aware that they are treated differently.

In addition, such technology may allow racial profiling.[75] The GDPR distinguishes between data revealing the racial and ethnic origin and processing of biometric data. For images, the recitals suggest that they shall only be considered biometric data if a biometric analysis is performed.[76] However, the wording "revealing racial and ethnic origin" suggests that the simple presence of such information in the image (e.g. skin colour) might be sufficient to make the data fall into the special categories of personal data, regardless whether this information is used or not. This ambiguity leads to an uncertainty which legal basis may be invoked and therefore for which purposes processing is permitted.

Allowing member states to create additional (different) legal frameworks for scientific research and statistical purposes with vague legal requirements for such laws, open to different interpretations (e.g. "respect essence of the right to data protection") consequently lead to a fragmentation of the data protection landscape. Questionable research methods may be applied in member states with the most permissive legal basis by using the free movement of personal data between the member states. Even if a conflict between national legislation and GDPR requirements is later found by the European Court of Justice, years of data processing based on the national legislation may then already have been performed.

Another issue may arise when sharing the raw biometric data through initiatives like the European Open Science Cloud (EOSC). Biometric data is tied to a natural person by its nature and therefore is hard to anonymize while still allowing for meaningful usage. There is a fundamental tension between GDPR principles like purpose limitation, storage limitation and goals of FAIR data like data reuse and accessibility. While the GDPR would advocate transparent and precise information on processing purposes and data retention, the principle of FAIR data aims to minimize restrictions and allow reuse for other studies.[77] This is especially problematic if commercial data reuse, as in the case of EOSC, is envisioned.[78]

2.9.3 Risk assessment and impact for research and innovation

Biometric information normally cannot be concealed or changed, creating a persistent privacy threat once obtained by any third party.[79] Especially troublesome in this regard is the process

[75] Id., p. 352 paragraph 123

[76] Recital 51 S 3 GDPR

[77] European Commission, Final Report and Action Plan from the European Commission Expert Group on FAIR Data, doi:10.2777/54599, p. 21

[78] European Commission, European Open Science Cloud (EOSC) Strategic Implementation Plan, doi: 10.2777/20237, p. 21

[79] Camisi P., Security and Privacy in Biometrics, Spinger, 2013, p. 69

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

of “function creep”, where the obtained data is repurposed for completely different uses than it was collected for. For example, biometric data obtained for health diagnostics research has the potential to later also be used in surveillance applications.[80]

New device categories may also be an important factor contributing to widespread deployment of biometric analysis. Especially in the field of speech-based emotion detection, training data annotated with expressed emotions is available only in sparse quantities.[81] Smart watches can measure biological indicators like heartbeat, blood pressure and oxygen levels in addition to voice recording. Combining these measurements with a small number of manually annotated data using semi-supervised learning techniques may lead to a much richer training data sets becoming available.[82]

This directly leads to the problem of covert biometric data analysis. While users are normally aware that they are providing biometric data when using fingerprint readers or iris scans, this is often not the case for audio or video captures.[83] Collection and distribution of such information is so widespread in messenger and social media apps that many users do not think twice before allowing access. It is therefore essential that the biometric processing as such is clearly stated and not cloaked away under generic terms like processing for research or developmental purposes. This is especially true for commercial research, where economic incentives may be intertwined with scientific research.

Allowing the member states to create additional legal frameworks for scientific data processing also runs the risks of initiating a downward competitive spiral, where member states have an incentive to lower the data protection standards to increase their attractiveness as a research location. It is therefore desirable to concretely define specific basis standards for ethical data processing, in order to at least partially bridge differences between national legislations. This applies in particular to EU projects, where researchers from a range of different member states may participate.

Even when originally developed for commercial applications, emotion detection technology may also be employed for national security purposes. In the context of research and innovation, it is therefore crucial to avoid linking the biometric information to individual identities as much as possible, collecting only the data absolutely necessary for the research in question. Otherwise

---

[80] Foundez-Tanuy M. et al, Biometric Applications Related to Human Beings: There Is Life beyond Security, *In:* Cognitive Computation 5(1), 2013, p. 147

[81] Yoon S. et al, Multimodal speech emotion recognition using audio and text. *In:* 2018 IEEE Spoken Language Technology Workshop (SLT). IEEE, 2018. p. 112

[82] Zhang Z. et al, Enhanced semi-supervised learning for multimodal emotion recognition, *In:* 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2016, pp. 5185, doi: 10.1109/ICASSP.2016.7472666.

[83] Zuo, H. et al. Covert photo classification by deep convolutional neural networks. *In:* Machine Vision and Applications 28, 2017. p. 623, https://doi.org/10.1007/s00138-017-0859-x

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

such research may be used as stepping stone to develop Orwellian technologies like mass mood surveillance of crowds.

It's also important to clearly communicate the research approach and basic assumptions of the research method. For example, within the recently popular field of machine learning and AI, skewed training data may result in an undesirable racial bias of the resulting emotion detection systems. Such a bias may be introduced entirely unwittingly, i.e. by using a training set which contains much more examples from one ethnic group than from others. In addition, machine learning does not only reflect existing societal bias or discrimination, it may also result in their amplification.

2.9.4 Mitigation measures

The development of ICT systems used for emotion detection requires large scale processing of biometric data. A data protection impact assessment (DPIA) for the concrete scientific data processing pursuant to the GDPR provisions must therefore be carried out.[84] It shall not be sufficient to simply refer to some abstract DPIAs provided by some member states for scientific research context,[85] as these necessary fail to capture the details of the concrete data processing situation.

Special attention should be paid to the principles of data minimisation and storage limitation. As biometric data by its nature is usually tied to an individual person, only the biometric features absolutely necessary to answer the research question shall be recorded and individual measurements deleted once the data processing for research is completed. The resulting analysis should be anonymized as soon as possible. Under no circumstances the data shall be processed with methods or for purposes which violate the principle of fairness and transparency enshrined in the GDPR.[86] The data should only be stored in encrypted form and only be available to the relevant researchers with access logging enabled.

2.10 AI and security

2.10.1 Context

The amount of data recorded by electronic devices has exploded in recent years. The ubiquity of smartphones and increasing use of connected IoT devices have led to many unseen volumes of data becoming available. Increasingly, automated approaches in the form of AI or machine learning are needed instead of explicitly programmed rules for each application to condense all this input into form suitable for further processing.

---

[84] Art 35 (3) b GDPR

[85] i.e. the DPIAs included in the annex of the Austrian „Forschungsorganisationsgesetz"

[86] Art 5 (1) a GDPR

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

As AI applications are developed in response to these classification and prediction tasks, voices demanding the use of this technology in the security context are becoming louder. However, the question has to be raised which particular type of security is sought in the specific context. As discussed in the section on the definitions of Security and Cybersecurity, there are strongly diverging meanings of security depending on the particular perspective of the research.

In the context of this discussion, national security shall encompass the protection of the overall social and legal system of a state against coordinated attacks. This is usually achieved by surveillance, detection and prevention of specific forms of unlawful activities. In contrast, social security shall ensure individuals an adequate standard of living by providing certain state services. This includes health services, pension and unemployment insurances.

2.10.2 Issue/gap

Ensuring a transparent decision-making process is one key requirement when using AI for security purposes. In the context of national security, being flagged by an automated system as potentially dangerous may have serious consequences for an individual. Because the decision-making process of AI algorithms is usually based on complex mathematical deductions, it may be difficult or impossible to obtain an explanation understandable by a human for the algorithmic result.

This is especially relevant since the right to data access is often limited in the context of national security and data is treated as confidential. For an affected person, it may therefore be difficult to find out why certain measures, e.g. frequent checks at airports, are performed.

In effect, it may become hard to distinguish whether a decision has been made by a human or by a machine. This is directly connected to the problem of responsibility in the AI context. Who is responsible if the decision made by an AI system is unlawful, e.g. discriminates against minorities? Is it the programmer who designed the system, the company which sold the system, the engineer who trained it, the employee who operated it or the legal person who procured it? What if the system itself is fair but the training data is biased? To ensure responsibility is assigned transparently such that a natural or legal person can always be held accountable for unlawful algorithms will be one of the major challenges of using AI in the security context.

2.10.3 Risk assessment and impact for research and innovation

One of the main risks of using AI for security applications the problem of false positives. In the context of social security, this may mean to be excluded from measures like training programs or state aid for continued employment. For national security, the consequences may be even more severe, ranging from denied visa, becoming a terrorist suspect, to prolonged time in jail because denied bail based on an AI algorithms decision.[87]

[87] https://www.theguardian.com/us-news/2018/sep/07/imprisoned-by-algorithms-the-dark-side-of-california-ending-cash-bail, accessed 25.09.19

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

In the context of cybersecurity, AI based intrusion detection systems react to unusual but legit behaviour with an alarm. In the case of intrusion prevention systems this may lead to automated restrictions or even shutdown of services for certain users.

The output of complex AI systems may create an illusion of completely objective, fact-based results. But even a small bias in the selected training data may lead to significantly biased results, especially if the system is enhanced by training data generated by its usage.

As an example, controlling people in certain neighbourhoods more frequently will lead to criminal activity being officially filed in this neighbourhood more often. Training the AI on this data would lead to the conclusion that the area has a higher criminality in comparison to other, less densely controlled neighbourhoods. This correlation may be misinterpreted as causal relation by the system. Without adequate countermeasures, an initial bias of the AI system may be amplified accordingly. This is further detailed in the section of AI and predictive policing. In the context of research and innovation it is therefore important to not only research AI algorithms but also criteria for robust, unbiased training data.

As negative decisions in both national and social security may have serious consequences for an individual, researches should keep the importance of explaining the system results human understandable way in mind. It is not enough to simply state the result, as this would effectively turn the result into a fact without exposing its foundations.

As AI models build on different training data may be repurposed for security applications, it is important to keep the limitations of the overall system in mind. Claims of high accuracy on a particular dataset in a highly controlled research environment may lead to unrealistic expectations on the performance of the system in the field. When assessing the usefulness of AI systems for a particular context, researches should always ensure representative training data from real world sources is used. Otherwise, the system may become fixated on irrelevant details, effectively “cheating” instead of performing the required task.[88]

In a security context, this might result in very dangerous situations. Imagine an AI algorithm for image analysis designed for recognizing street signs. If a maliciously crafted input, say by applying small scale graffiti to a speed limit sign, changes the AI interpretation of the speed limit to a stop sign, passing traffic may suddenly perform an emergency break.[89] When using data gathered from an uncontrolled environment, AI researchers should always consider the risk of deliberate tampering with their input. When assessing AI algorithms for security applications, the importance of having robust, tamper resistant result should not be underestimated.

[88] https://techcrunch.com/2018/12/31/this-clever-ai-hid-data-from-its-creators-to-cheat-at-its-appointed-task, accessed 25.09.19

[89] Eykholt K. et al, Robust Physical-World Attacks on Deep Learning Visual Classification, at CVPR 2018

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

The risk of tampering also exists the other way around. AI algorithms can generate fake video footage which may be perceived as genuine content by humans. In the context of the so called "deepfakes" videos, the footage of political speeches may be altered by dubbing with a new script while convincingly synchronizing facial movements accordingly.[90] Or the face of a porn actor convincingly be swapped with a celebrity appearing in a compromising position.[91] The abusive potential of such technology is vast, as the required tools to fabricate such fakes are widely available.[92] If undetected, such technology may allow malicious parties to question the credibility of genuine content while producing fake content at the same time, putting the reliability of video footage in general in question.

2.10.4 Mitigation measures

Many risks of using AI result from individual results of the algorithm being incomprehensible for human assessment and potential correction. Approaches like "explainable AI" aim to change that by requiring the results to be understandable for humans. These systems strife to provide the benefits of AI while making the resulting system for transparent and therefore accountable. Requiring such properties from AI systems used in national and social security may create incentives for further development of such systems.

As an additional benefit, this may also help to expose biases resulting from unrepresentative or incomplete training data sets. Traceable usage of discriminatory criteria like skin colour or ethnic after training the AI may provide hints that the data set is biased. Ideally, representative training data sets should be vetted and standardized to allow fair comparison of the AI systems performance

Statistical tests for specific criteria like age or gender discrimination may also help to expose possible selection bias being present in the training data of AI systems. However, such tests are necessarily incomplete as they only expose certain discrimination and do not provide insides into the inner workings of the AI algorithm. Wherever possible they should therefore be combined with "explainable" AI systems for further transparency.

Finally, an honest communication of the strengths and weaknesses of current AI systems contribute to a realistic assessment of the technology for a particular application. While modern AI systems may perform much better than traditional technology in some fields, they should

[90] Vincent J, https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed, accessed 24.10.19

[91] Kharpal. A, https://www.cnbc.com/2018/02/08/reddit-pornhub-ban-deepfake-porn-videos.html, accessed 24.10.19

[92] AFP, https://www.theguardian.com/technology/2019/sep/02/chinese-face-swap-app-zao-triggers-privacy-fears-viral, accessed 24.10.19

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

not be seen as a panacea readily applicable anywhere, especially if the decision process is not traceable by humans.

In summary, and essential objective of (research into) mitigation measures is to contribute to "meaningful human control"[93] and "meaningful opportunity for human choice"[94] to secure human oversight, moral responsibility and legal accountability. In the context of cybersecurity, awareness about the NIS Directive[95] and AI related current activities by ENISA[96] should be raised among the ICT researchers' community.

2.11 AI for predictive policing

2.11.1 Context

There has been a visible shift in the last decades from post-crime towards pre-crime.[97] With the use of big data and accessible analytical methods, pre-crime strategies are becoming ever more popular. More and more law enforcement agencies around the world have adopted predictive policing technologies, i.e. a broad range of algorithmic and data-driven practices and software tools[98] to guide their decision-making. The more specific aims of using such practices and tools is to predict where (e.g. in what geographic areas) and when crimes may happen or who may be involved in a crime (either as an offender or a victim) so that police and social service providers can make better use of their current resources. Unlike traditional strategies that focus on responding to crime ex post, the major aim of pre-crime strategies is to prevent crime ex ante.

Although there is no single agreed definition, two key components of predictive policing are commonly mentioned: firstly, a broad variety of types of data is used, and, secondly, police takes action before possible criminal activities occur so as to prevent crime from happening.[99]

Numerous legal instruments are relevant in the governance of predictive policing. The Universal Declaration on Human Rights, the European Convention of Human Rights and the

[93] European Group on Ethics in Science and New Technologies. (2018). Statement on Artificial Intelligence, Robotics and 'Autonomous' systems. Retrieved September, 18, 2018.

[94] High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI.

[95] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[96] https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence

[97] Rosamunde van Brakel & Paul De Hert „Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology-based strategies", 2011, p.165.

[98] Peter M. Asaro: AI Ethics in Predictive Policing: From Models of Threat to an Ethics of Care. https://dblp.org/db/journals/tasm/tasm38.html" \l "Asaro19: 43 (2019)

[99] Albert Meijer & Martijn Wessels (2019) Predictive Policing: Review of Benefits and Drawbacks, International Journal of Public Administration, 42:12, 1031-1039, DOI: 10.1080/01900692.2019.1575664

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

EU Charter of Fundamental Rights all contain important commitments to human rights. The General Data Protection Regulation (EU) 2016/679, the Data Protection Directive for Police and Criminal Justice Authorities (EU) 2016/680, and the respective national laws (e.g. laws on data protection, law on police) set out important principles and standards governing the rights to privacy and data protection. The jurisprudence of the European Court of Human Rights and the Court of Justice of the EU as well as national courts give guidance on how the legal doctrine on human rights should be developed as well as how the set principles and standards should be applied in practice. The modernised Data Protection Convention No.108 of the Council of Europe specifically addresses issues surrounding big data applications.

Although the use of predictive policing technologies might potentially yield benefits (e.g. improved accuracy, reduction of costs, reduction of crime), there are important ethical concerns, too.

2.11.2 Issue 1

The central ethical concern in predictive policing is that law enforcement officers, relying on predictive policing technologies, could treat individuals likely to become involved in crime according to the technology's predictions in the same way as offenders who have committed a crime. This also uncovers more general problems common to all predictive systems: Firstly, the predictions are based only on statistically significant correlations without necessarily establishing causality. Secondly, the probabilities are calculated based on historical data. Therefore, conclusions drawn from these extrapolations assume that the future will closely resemble the past. Hence, predictive policing may not only foster biases and prejudices, but also prevent alternative futures from emerging.

2.11.3 Risk analysis and impact for research and innovation

Moreover, prejudging individuals may effectively violate the presumption of innocence. The presumption of innocence is widely recognized as the fundamental principle in criminal justice. The idea behind this principle is that one is considered innocent unless proven guilty. So, if a person has not (yet) committed a crime (or can be proven guilty of preparing a criminal offence), he or she cannot be held liable. This principle is envisaged in the main international and regional human rights treaties, like Universal Declaration on Human Rights (Article 11(1)), European Convention of Human Rights (Article 6(2)), and the EU Charter of Fundamental Rights (Article 48(1)).

Using predictive policing technologies threatens to undermine the presumption of innocence and, therefore, can disrespect human dignity as well as the fundamental rights of individuals. This is particularly relevant with regard to predictive profiling. Predictive profiling refers to the practice of ranking individuals and groups of people according to their calculated propensity to commit or become involved in crime. Commonly used criteria to calculate such propensities are behavioural data and population level characteristics (e.g. demographic data like ethnicity, religion, nationality). Based on the calculated propensities, allegedly likely offenders are then

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

more often stopped, searched or arrested. Searching alleged offenders more often will most likely lead to a higher conviction rate in the targeted group, since more offences are noticed by police officers which would otherwise go unnoticed. This higher conviction rate may lead machine learning systems to label the group as potential offenders, leading to a feedback loop amplifying pre-existing prejudices. Collecting data and flagging individuals using predictive policing tools casts a shadow of mistrust over innocent people, threatens their privacy, as well as stigmatizes and discriminates those who are ranked as potential offenders and their communities.

2.11.4 Mitigation measures and costs

Normatively, law enforcement should be designed to best serve communal and societal needs. Although predictive policing technologies pose risks, prohibiting their use entirely is not a promising strategy, as it risks foregoing benefits big data might yield. However, these technologies should be introduced in a responsible and cautious manner in order to avoid undermining basic rights and established principles of justice. In cases of doubt, the use of such technologies should not be allowed.

The development and introduction of predictive policing technologies should be based on a number of considerations. First of all, the technology should be necessary to increase communal security and proportionate, i.e. less intrusive alternatives capable of achieving the same aims should be absent and likely benefits of the predictive policing technology should outweigh risks. This presupposes a proper risk assessment that includes the evaluation of risks increased community and individual surveillance gives rise to, increased risks of unfair treatment, risks to privacy and other fundamental rights violations.

Moreover, risk assessments should be conducted as transparently as possible. The key element of transparency is the disclosure of how the technology will generate the desired outcome (what data it collects, for what purposes it will be used, which analytic methods will be used to process data and produce the result) and how law enforcement agencies will use the outcome in their work. For instance, a suspect is usually entitled by national police laws to demand an explanation why he or she is charged. This right is threatened whenever satisfactory, humanly intelligible explanations cannot be given because algorithms used in predictive policing remain obscure. Hence, transparency is of utmost importance to allow this right to be exercised.

Involvement of local communities is also crucial to build confidence and trust that the technologies will be used in a beneficial way and that legitimate concerns will be alleviated as much as possible.

Transparent risk assessments should not only be performed in the creation phase by developers, researchers and regulatory bodies, but also during the implementation phase by the users of the technology, because hitherto unforeseen risks and problems might arise. In other words, dynamic technological developments require continuous risks assessments. To ensure the ability to carry out such risk assessments, training of assessors (who are in many cases from the technological background) is necessary to address the ethical and legal issues successfully.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.11.5 Issue 2

The second major issue in predictive policing is insufficient awareness of what technologies can reasonably be expected to accomplish in accurately predicting crime. Developers and users of such technologies often tend to assume that algorithms are based on accurate, complete and relevant data. However, as many examples show, this is not always the case.[100]

2.11.6 Risk analysis and impact for research and innovation

One of the features of the predictive policing (as well as of many other applications of big data), is that it involves the collection of large quantities of data, including personal data. Data usually are collected by different actors, in different formats and contexts, as well as from multiple sources. Datasets used in predictive policing thus may comprise data from past crimes as well as data from state-run databases and other big data sources. Combining data from multiple sources and using data collected for various other purposes increases the risk of inaccuracy and latent bias. Consequently, seemingly objective or neutral data might in fact be highly problematic on closer inspection. To the extent predictive policing technology is built on such data, there is an increased risk of further significant negative impacts on policing practices because algorithmic predictions and amplification of biases might not only violate the presumption of innocence, but also make false predictions. Whenever this is the case, the technology becomes ineffective and even discriminatory.

2.11.7 Mitigation measures and costs

Different mitigation measures are conceivable. As for existing predictive policing technologies, research assessing their effectiveness, impacts on society and democratic principles is crucial. As for all, including future technologies, research needs to promote critical understanding among predictive policing developers, users and regulatory bodies to better understand what data are needed to develop effective technologies, what limitations and vulnerabilities (e.g., what biases it may contain) these technologies inadvertently have and how to reduce them. It should address as well how the use of technologies affects the practices of users (i.e. police and other law enforcement agencies), those affected by the outcome of the use of these technologies (i.e. citizens and the society as a whole). Due to the limitations and vulnerabilities of the algorithms, it is also important to ensure that law enforcement agencies' actions are not based exclusively on automated decisions, but are always only an aid to decisions taken by human professionals after a careful and detailed analysis of existing evidence. In addition, human beings must continue to be able to impose themselves on intelligent automated systems, taking

[100] Richardson, Rashida and Schultz, Jason and Crawford, Kate, Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice (February 13, 2019). New York University Law Review Online, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3333423.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

their decisions autonomously, having all the necessary reports on display, within the framework of the free appreciation of evidence, which must not be renounced. The judicial and procedural systems must ensure that this is the case.[101]

Due to evolving nature of analytical tools and methods and technological complexity of the predictive policing tools, regular training of those involved in developing and using those tools must be ensured. In addition, domain experts should be involved in research and innovation processes in order to help developers understand the context in which technologies will be used and enable them to better anticipate potential misuses ex ante.

Also, in order to avoid the scenario of collecting any and all available data in the hope that something useful will turn out from them, particular attention should be paid to the data minimisation principle, demanding that personal data should be limited to what is really necessary to achieve stated aims. Given the nature of big data and its broad range of possible uses, application of data minimisation becomes very challenging in general; specific research on how GDPR interprets this principle in big data field would be crucial.

2.12 Security standards for IoT devices

2.12.1 Context and legal background

More and more devices, not primarily used for connected activities, gain Internet access today to make our lives easier and more comfortable. Doing so, these so-called Internet of Things (IoT) devices have access to our home- or office-networks and are dealing with sensible personal data that controls great parts of our lives.[102] Consequently, an effective protection from unauthorized accesses to these devices is required as well as a protection of the collected data. However, as they have less computing capacity, IoT devices are poorly equipped with security measures.[103] By today there have already been several attacks on IoT.[104]

Until now, no holistic and mandatory security standards for IoT devices have been legally enacted. Many organisations working on cybersecurity or network security have published Codes of Practice for IoT, addressing either manufacturers or users of IoT devices. The first

[101] Casabona, C. M. R. (2018). Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad. Revista de Derecho, Empresa y Sociedad (REDS) (13), 39-55.

[102] Schneier, B. (2018). New IoT Security Regulations. Retrieved from https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html

[103] Towers-Clark, C. (2019a). IoT Security Must Evolve To Survive. Retrieved from https://www.forbes.com/sites/charlestowersclark/2019/06/14/iot-security-must-evolve-to-survive/#6a11385635c1

[104] Daube, N. (2019). Regulating the IoT: Impact and new considerations for cybersecurity and new government regulations. Retrieved from https://www.helpnetsecurity.com/2019/04/11/iot-regulation-2/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

legislator tackling the absence of legally binding rules was California in 2018 with its SB-327 law, which will take effect in 2020.[105] According to this law, every sold IoT product in California needs reasonable security features.[106] A different approach was taken in the US legislation. After two failed bills in 2017 and 2018 a third bill called IoT Cybersecurity Improvement Act of 2019 regarding security of IoT products purchased by the US government was introduced to senate.[107] The IoT Consumer TIPS Act of 2017 aims to develop educational resources for consumers[108] whereas the SMART IoT Act foresees a study to describe the state-of-art US IoT industry[109]. Similarly, to the SMART IoT Act of the US, Japan is testing default credentials to log into Internet connected devices without notifying owners to challenge the security of their devices.[110] This project shall give an overview about how many weakly secured devices are connected to the Internet and inform the owners to disconnect them.

In Europe, the UK has published a Code of Practice in 2018 for all parties involved and is now consulting on regulation prospects.[111] In the future, this shall lead to a labelling system, ensuring a mandatory minimum of security for every IoT device in the UK.[112] The European Union has passed the EU Cybersecurity Act in 2019, leading to a stronger mandate for ENISA and a cybersecurity certification framework.[113] ENISA already published Baseline Security Recommendations for IoT as has ETSI, which published TS 103 645 Cyber Security for

---

[105] Lindsey, N. (2019). New IoT Security Laws Seek to Protect Consumers From Hacks of Internet-Connected Devices Magazine. Retrieved from https://www.cpomagazine.com/data-protection/new-iot-security-laws-seek-to-protect-consumers-from-hacks-of-internet-connected-devices/

[106] California State Senate (2018). Senate Bill No. 327.

[107] Gallo, M. N., & Goodloe, K. (2019). Senate Reintroduces IoT Cybersecurity Improvement Act. Retrieved from https://www.insideprivacy.com/internet-of-things/senate-reintroduces-iot-cybersecurity-improvement-act/

[108] Senate of the United States (2017). S. 2234.

[109] Senate of the United States (2018). H. R. 6032.

[110] Boyd, J. (2019). Japan To Probe IoT Devices And Then Prod Users To Smarten Up: A government project begins testing millions of Internet-connected devices to see how safe they are from cyberattacks. Retrieved from https://spectrum.ieee.org/tech-talk/telecom/internet/japan-aims-to-probe-unsecured-iot-devices-and-then-prod-users-to-smarten-up

[111] U.K. Department for Digital, Culture, Media & Sport. (2019). Secure by Design: The Government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home. Retrieved from https://www.gov.uk/government/collections/secure-by-design

[112] Towers-Clark, C. (2019b). UK To Introduce New Law For IoT Device Security. Retrieved from https://www.forbes.com/sites/charlestowersclark/2019/05/02/uk-to-introduce-new-law-for-iot-device-security/#477bce61579d

[113] Schmidt, J. (2019). EU-Parlament stimmt über Cybersecurity Act ab. Retrieved from https://www.elektronikpraxis.vogel.de/eu-parlament-stimmt-ueber-cybersecurity-act-ab-a-808711/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Consumer Internet of Things, a standard without legal force.[114] All in all, the engagement in law-making for IoT devices by governments is rather restrained.

2.12.2 Issue

Security standards for IoT devices are a legal gap. There is no law in the EU or its member states setting mandatory requirements for IoT device security, nor is there a law which could be applied analogously, at least as long as no personal data are concerned.[115]

2.12.3 Risk assessment & impact for research and innovation

The lack of mandatory security standards for IoT devices are a high potential risk. They regulate great parts of our lives like TVs, washing machines, thermostats, but also pacemakers or smart grids. Concludingly, these devices have access to our private information and are also generating sensitive data. Because of the high frequency in which new IoT device are brought to market, manufactures need to keep prices low – and therefore want to avoid huge investments in security. Consumers are often unaware of the lacks in privacy and security caused by these devices. Furthermore, the little computational capacity of IoT devices inhibit common security technologies. A fact that is already abused for cyberattacks. Consequently, a legally binding security by design approach is needed.

This is highly relevant for researchers, dealing with IoT devices, since they have to guarantee the security of their processed data by law (compare Art. 32 GDPR).

2.12.4 Mitigation measures and costs

To mitigate these risks, adopting a mandatory minimum of requirements for security standards is necessary. Organisations of cybersecurity or network security have developed a number of Codes of Practice which can give an orientation about measures that are already applicable today. A labelling system as aim for in the UK gives for instance simple information about the privacy impact of an IoT device similar to the EU energy efficiency labelling system. This could go along with consumer education about IoT and privacy aspects of IoT devices. IoT devices are sold and produced worldwide, hence the problem should be addressed internationally and not only on an EU level and security standards should be applicable worldwide.

---

[114] European Telecommunications Standards Institute (02.2019). CYBER; Cyber Security of Consumer Internet of Things. (TS 103 645).

[115] Art 32 GDPR requires the implementation of “appropriate technical and organisational measures to ensure a level of security appropriate to the risk”.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039.

2.13 Insufficient guidance to participants in open science

2.13.1 Context and legal background

Open Science is one of the goals of the EC's research and innovation policy[116]. It is an ongoing transition in how research is performed and how knowledge is shared[117]. One aspect of open science is to provide open access[118] to scientific research data following the FAIR principle[119,120,121]. FAIR means to make research data ***f****indable*, ***a****ccessible*, ***i****nteroperable* and ***r****eusable* (FAIR)[122]. However, insufficient guidance is available to participants on how to treat personal data in open science and the open research data pilot.

As of the Work Programme 2017 the Open Research Data pilot is extended to cover all thematic areas of Horizon 2020 per default[123,124]. The obligation of providing open access to research data is described in Article 29 of the Grant Agreement[125]. In particular, Article 29.3 is concerned with the obligation to provide open access to research data. Article 29.6 outlines the consequences of non-compliance, including a possible reduction of the grant and a referral to chapter 6 that, among others, describes sanctions, damages, suspension, and termination.

Article 29.3 addresses the case of personal data by stating that "This does not change the obligation to protect results in Article 27, the confidentiality obligations in Article 36, the security obligations in Article 37 or the obligations to protect personal data in Article 39, all of which still apply". The referenced article 39 states in its letter 2 that "The beneficiaries must process personal data under the Agreement in compliance with applicable EU and national law on data protection (including authorisations or notification requirements)."

---

[116] https://ec.europa.eu/info/research-and-innovation/strategy/goals-research-and-innovation-policy_en

[117] https://ec.europa.eu/research/openscience/

[118] https://ec.europa.eu/research/openscience/index.cfm?pg=openaccess

[119] https://publications.europa.eu/en/publication-detail/-/publication/7769a148-f1f6-11e8-9982-01aa75ed71a1/language-en/format-PDF/source-80611283

[120] https://www.force11.org/group/fairgroup/fairprinciples

[121] https://www.nature.com/articles/sdata201618

[122] See https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf on page 3.

[123] See https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm in Horizon 2020 Open Research Data Pilot and Data Management Plan, Scope of the pilot.

[124] https://ec.europa.eu/research/press/2016/pdf/opendata-infographic_072016.pdf

[125] See https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf on page 245 in H2020, Chapter 4, Section 3, Subsection 3, Article 29.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

The wording "This does not change the obligation to protect personal data in Article 39" gives the impression that data protection is an additional obligation, not that data protection is a valid reason to wave the obligation to provide open access to one's research data. The latter interpretation can only be found in the annotation[126] of the grant agreement (which in itself lacks legal significance) in the info box on page 251. In particular, the text of the box includes the following: "Participation is therefore now in principle the default. However, actions may opt out at any stage […] if […] participation is incompatible with rules on protection of personal data". In the context of Article 39.2, the annotation then refers to "Directive 95/46/EC" instead of the GDPR that supersedes this directive.

A search for additional information on how to deal with personal data when facing the obligation to provide open access to research data in Horizon 2020 fails to produce clear results. For example, the "Guidelines on FAIR Data Management in Horizon 2020"[127] lack a section on personal data and fail to describe the protection of personal data as a valid reason for opting out. The document mentions "personal data" solely in section 5 of Annex 1 "Ethical aspects", giving the legally unstainable impression that just some "informed consent" was sufficient to permit open access to personal data without further detailing specification (see the following paragraph).

In more detail, this mentioned sentence reads as follows: "Is informed consent for data sharing and long-term preservation included in questionnaires dealing with personal data?" To researchers who lack legal expertise, this gives the impression that mentioning data sharing in the consent renders it legal to provide one's data to other researchers who process them in turn. This understanding is legally problematic. Among the issues are the following:

- Due to the "coupling prohibition" of Article 7(4) GDPR, it is not possible to use a single consent for both, the processing of data by the primary controller and the "sharing". Much rather, two distinct consent requests are necessary that render it possible that a data subject agrees with the primary processing, but refrains from granting consent to "sharing".
- While consent to "sharing" can provide a legal basis (namely Article 6(1)(a) GDPR) for the disclosure of data to secondary controllers (i.e., third party recipients according to Articles 4(9) and (10) GDPR), it fails to provide a legal basis for the processing activities pursued by such secondary controllers. While it is theoretically possible for a primary controller to ask consent for the processing by a secondary controller, this is only valid if the secondary controller is identified to the data subject (see Recital 42 GDPR). Considering that this would require a separate consent request for each participating secondary controller and that all secondary controllers be known at the time of asking consent, this is practically rather difficult. Whether a primary controller

[126] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf

[127] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

can request consent for the processing of a yet unidentified secondary controller is currently unclear (see Issue 2.2 “Collecting Consent for a Yet Unidentified Secondary Controller” above).

- To be GDPR-compliant, even when sharing personal data, data subject rights have to be implemented. A valid solution to “sharing” of personal data must therefore address the problem of how data subjects can request their rights (e.g., though a single point of access) and how such requests are propagated across all participants of the “sharing”.

Comparable to the “Guidelines on FAIR Data Management in Horizon 2020”, also the guidance in the context of OpenAIRE is insufficient and misleading. It is telling that the link to “About personal Data”[128] on the page “Open Research Data the New Norm in H2020”[129], under “Information at the OpenAIRE portal” results in “Bad karma: we can't find that page!”. Much of the information found by Google under “OpenAIRE personal data” is erroneous or misleading. For example, the “Guides for Researchers--How to deal with sensitive data”[130] states that “For personal data fully informed consent should be given for collecting, processing and storing data”. This is equally simplistic and misleading as the above discussed guidance in “Guidelines on FAIR Data Management in Horizon 2020”. While the “Fact Sheet on Personal data and the Open Research Data Pilot”[131] correctly states that “The best way to fulfil the requirements of the Open Research Data Pilot and data protection rules at the same time is to anonymise personal (research) data before making them openly available”, it also states that “another way to guarantee compliance with data protection rules is to obtain the consent of the data subject to use and exchange their data”. Again, the legal shortcomings discussed above apply.

OpenAIRE also provides an online tool[132] for the anonymization of personal data. Unfortunately, it lacks any legal analysis on how to use it in compliance with the GDPR. Open questions include what legal basis researchers have to upload not-yet-anonymized data to the service, what legal basis the service has for its processing of personal data, whether the service is a controller, joint-controller, or a processor, what technical and organizational measures are in place to comply with data protection, for how long the service stores the received personal data, whether a data protection impact assessment is available, or who the responsible data protection officer of the service is.

[128] https://www.openaire.eu/personal-data-and-the-open-research-data-pilot

[129] https://www.openaire.eu/open-research-data-the-new-norm-in-h2020

[130] https://www.openaire.eu/sensitive-data-guide

[131] https://www.openaire.eu/factsheet-personal-data

[132] https://amnesia.openaire.eu/

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039.

2.13.2 Issue

The current governance of open science and particularly open access to scientific research data in Horizon 2020 provides insufficient and misleading guidance to researchers and programme participants on how to deal with personal data. It gives the erroneous impression that providing open access to such data was mandatory and that non-compliance results in dire consequences. There is insufficient clarity that opting out of open access in the case of personal data is mandatory to comply with the GDPR. The available guidance on how open access fits with personal data is overly simplistic and misleading (see above). Tools provided in the context of open access lack the necessary legal components.

2.13.3 Relevance and impact on ICT R&I

The shortcomings of governance in the area of open access and personal data risk to push researchers and programme participants to violate requirements of the GDPR and thereby become subjected to action by data protection supervisory authorities or by courts. This may include fines. These kinds of incidents risk to discredit open science and open access efforts.

2.13.4 Mitigation measures and costs

The following actions are recommended to mitigate the issue:

- Improvement of the wording of Gant Agreements.
- Update of the Annotation of the Grant agreement (e.g., to reference the GDPR instead of the directive).
- Clear, prominent and consistent guidance on how to deal with personal data in the relevant documents for programme participants including (but not limited to) the Horizon 2020 *Data Management page*[133], the *Guidelines on FAIR Data Management in Horizon 2020*[134], and the material provided by OpenAIRE.
- Rephrasing of misleading advice, as for example that consent is sole basis for open access to personal data and supplementing consent requirements, necessary safeguards as well as pointing to alternative option as legal basis.
- Implementation of the necessary legal components in the online anonymization service of OpenAIRE.

The cost of the recommended actions is estimated to be relatively low.

[133] https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm.

[134] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.14 Sharing of personal data in Open Science fails to be considered to its full potential

2.14.1 Context and legal background

Open Science is one of the goals of the EC's research and innovation policy[135], but fails to be considered to its full potential. It is an ongoing transition in how research is performed and how knowledge is shared[136]. One aspect of open science is to provide open access[137] to scientific research data following the FAIR principle[138,139,140]. FAIR means to make research data ***f****indable*, ***a****ccessible*, ***i****nteroperable* and ***r****eusable* (FAIR)[141]. As of the Work Programme 2017 the Open Research Data pilot is extended to cover all thematic areas of Horizon 2020 per default[142,143].

In a wide range of scientific disciplines, research data include personal data. This is for example the case in medicine, social sciences, economics, and the management of resources consumed or controlled by humans (e.g., in energy, mobility, or smart cities). Due to data protection requirements, it is not possible to directly grant open access to personal data[144]. There are two options to share such data anyhow in the scientific community:

- Anonymization of personal data prior to granting open access.
- "Targeted sharing"[145].

The former option eliminates all possibilities that the data can identify natural persons and thus removes them from the realm of personal data and the applicability of the GDPR. As non-

[135] https://ec.europa.eu/info/research-and-innovation/strategy/goals-research-and-innovation-policy_en.

[136] https://ec.europa.eu/research/openscience/.

[137] https://ec.europa.eu/research/openscience/index.cfm?pg=openaccess.

[138] https://publications.europa.eu/en/publication-detail/-/publication/7769a148-f1f6-11e8-9982-01aa75ed71a1/language-en/format-PDF/source-80611283.

[139] https://www.force11.org/group/fairgroup/fairprinciples.

[140] https://www.nature.com/articles/sdata201618.

[141] See https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf on page 3.

[142] See https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm in Horizon 2020 Open Research Data Pilot and Data Management Plan, Scope of the pilot.

[143] https://ec.europa.eu/research/press/2016/pdf/opendata-infographic_072016.pdf

[144] https://www.openaire.eu/factsheet-personal-data

[145] This term is used by OpenAIRE in their fact sheet on "Personal data and the Open Research Data Pilot" (see footnote above)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

personal data, anonymized data can be shared in a FAIR open access scheme like other research data.

The latter option is recommended for personal research data where anonymization is not possible. This is for example the case with individual-level de-identified data where open publication (that enables processing by anyone, for any purposes including re-identification) bears excessive risk of at least selected individuals being identified based on the data themselves. Here, in order to limit the risks to the rights and freedoms of the involved natural persons, the FAIR principles have to be applied in an appropriate manner.

This concerns in particular the R (re-usable) and the A (accessible) of FAIR. For example, re-use, i.e. processing of personal data, requires a legal basis[146] (see Article 6(1) GDPR). Parties who re-use the data in possession of such a legal basis, i.e., "secondary controllers", may need to limit their processing to specific purposes (e.g., those specified in the consent (see Article 6(1)(a) GDPR) or compatible purposes such as scientific research (see Articles 5(1)(b) and 6(4) GDPR) and guarantee that certain safeguards (see for example Article 89(1) GDPR) and safety measures (see Article 32 GDPR) are in place. Evidently, this limits the eligible parties who can get access to the personal data. While the accessibility principle (A) of FAIR[147] can still be satisfied, strong emphasis has to be put on the criterion A1.2 regarding authentication and access control. The reusability principle (R) of FAIR is no longer applicable as is. In particular, the criterion R1.1 that requires a "data usage license" is not applicable since usage licenses are based in copy-right law and lack an equivalent in data protection law. Instead, in data protection, the "conditions of use" likely take the form of a legal construct similar to a contract between controller and processor.

While open access of anonymized data seems to be well understood and supported by authoritative guidance[148] and even some tools[149]; the mechanisms and legal constructs for applying FAIR to personal data yet remains unclear. This is for example evident in the guidance provided on targeted sharing the OpenAIRE fact sheet[150], that gives the legally unsustainable impression, that consent was sufficient[151] to enable such data sharing. The conditions under which external open access infrastructure can be used also require analysis and clarification.

---

[146] See also the issue that asks for the clarification whether consent can be asked for yet unknown third parties.

[147] https://www.go-fair.org/fair-principles/

[148] Article 29 Data Protection Working Party, WP216, Opinion 05/2014 on Anonymisation Techniques, Adopted on 10 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, last visited 25/09/2019.

[149] For example, https://amnesia.openaire.eu/ (but note that the legal analysis of how to use in particular the online version of the tool in a GDPR-compliant manner seems to be missing).

[150] https://www.openaire.eu/factsheet-personal-data

[151] See Footnote 17 above. See also footnote 33 above that illustrates that the legal situation is currently unclear and that authoritative interpretation of the GDPR on this point is necessary.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.14.2 Gap

How to share personal scientific research data in an open science / FAIR open access context is currently not sufficiently understood. Legal mechanisms for such sharing—roughly equivalent to the "data usage licenses" addressed in FAIR's R1.1—are missing.

2.14.3 Risk assessment and impact on ICT R&I

In a wide range of scientific disciplines, research data include personal data (see examples above). Due to the gap, only the small percentage of this data that can successfully be anonymized can be shared in an open science / FAIR open access approach; the remainder of this data is excluded from the open science approach. This means that the open science / FAIR open access approach is not yet used to its full potential and that its benefits cannot be harvested in research areas that typically deal with personal data. As a consequence, these research areas remain less cost effective and the innovation boost promised by open science fails to materialize.

2.14.4 Mitigation measures and costs

The following actions are recommended to close the described gap:

- Develop set of reusable procedures and legal mechanisms (roughly equivalent to the "data usage licenses" addressed in FAIR's R1.1) for FAIR open access of personal data[152].
- Validate these in a wider circle such as a hearing process.
- Disseminate the found procedures and mechanisms in the research community and to programme participants.
- If possible, create support for these procedures and mechanisms in existing open access infrastructure.
- Establish the procedures mechanisms as global standard, comparable to creative commons licenses. This step is crucial since a proliferation of similar but different procedures and mechanisms may prevent the aggregation of data sets[153] due to incompatibility.

The cost of the first proposed action that creates a better understanding of the situation and proposes a first version of procedures and legal mechanisms is limited[154]. The outcomes of this first step can be used as stage gate to decide on additional actions that may come at a somewhat higher cost.

---

[152] Note that the PANELFIT project plans to work on this issue.

[153] Note that aggregation is often necessary from smaller geographical units where data are typically collected to larger ones in order to get the "big picture".

[154] In particular when considering that the already financed PANELFIT project will work on this gap.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

3 Conclusion

The critical analysis of security and cybersecurity ELI in the context of ICT research and development identified a large number of issues and gaps, not surprisingly pertaining to a very broad range of domains. Security, and to a lesser degree also cybersecurity, are multidimensional terms with distinct meanings and priorities attributed to the subdimensions by different individuals or groups. Security objectives may, at least at a first glance, be in conflict with other human rights and values, a fact that also became visible during the debate on the use of surveillance technologies in the context of the Covid19 pandemics.

The identified topics reached therefore from the need of more clear definitions and debates to the complex relationships between the sometimes conflicting values, impacts of ICTs on humans and the economic, political and social systems they live in, over security threats related to global shifts in ICT related economic powers to ethical and legal issues related to emerging ICTs.

This analysis provides a rich basis for future reports of the PANELFIT project, addressing issues and gaps that are relevant for ICT research and development in general and in particular for the use of advanced ICT in the context of security and cybersecurity, identifying topics that are important on a national or EU governance level, and raising crucial questions that urgently need to be tackled on a global level.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Appendix: List of participants

J. Peter Burgess, Ecole Normale Supérieure, Paris

Professor and Chair of Geopolitics of Risk at the Ecole Normale Supérieure, Paris and Adjunct Professor at the Center for Advanced Security Theory (CAST), University of Copenhagen. He is also Series Editor of the Routledge New Security Studies collection.

Soheil Human, Vienna University of Economics and Business (WU Wien)

Director of the Sustainable Computing Lab (http://sustainablecomputing.eu) at WU Wien. He has an interdisciplinary and mixed background in Artificial Intelligence (AI), Cognitive Science, History and Philosophy of Science (HPS) and Science-Technology-Society (STS).

Alena Pejcochova, Czech Republic National Police

PhD graduate from the Police Academy of the Czech Republic, graduate from the University of Nottingham (M.A. in International Security and Terrorism). Besides university teaching she is working at the Czech Republic National Police, focusing on cybercrime.

Aurélie Pols, Data Protection Officer, Privacy Engineer, and Data Scientist in Madrid, Spain

Lecturer at the Data Protection Officer (DPO) Certification Course held by the Maastricht University. She is also a member of EDPS' Ethics Advisory Group (EAG) and co-chair of IEEE's P7002 initiative on Data Privacy Process standards.

Maria Grazia Porcedda, School of Law at Trinity College Dublin

Assistant Professor of IT Law at the Trinity College Dublin. Amongst other positions she was a Research Fellow at the University of Leeds, a Research Associate within the Robert Schuman Centre for Advanced Studies and at the European University Institute in Florence.

Charles D. Raab, University of Edinburgh

Professorial Fellow, Politics and International Relations, School of Social and Political Science, The University of Edinburgh; and Fellow of the Alan Turing Institute. He is also a Director of CRISP (Centre for Research into Information, Surveillance and Privacy) and a founder of the Scottish Privacy Forum.

Ivan Szekely, Central European University

At present he is Senior Research Fellow at the Vera and Donald Blinken Open Society Archives at Central European University, associate professor at the Budapest University of Technology and Economics, and board member of the Eotvos Karoly Policy Institute.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.