D2.3

Key challenges and promising solution approaches

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D2.3 / V1.0
Work package contributing to the deliverable	WP2
Due date	January 2021 – M24
Actual submission date	1st February 2021

Responsible organisation	MRU
Editor	Regina Valutyte
Dissemination level	PU
Revision	V1.0

Abstract	This deliverable presents the research of key challenges related to a subset of the aspects identified in the previous report. The issues are first of all related to the application of GDPR. They also cover the concept of Responsible Cybersecurity Research and Innovation, contents and limitations of Security and Public Order criteria under EU Investment Framework Regulation, and legal regulation of disinformation.
Keywords	ELSA, GDPR, national security, Coordinated Vulnerability Disclosure, Responsible Cybersecurity Research and Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Regina Valutytė (MRU)

Contributors (ordered according to beneficiary numbers)

Michael Friedewald, Ralf Lindner, Thomas Jackwerth-Rice (Fraunhofer)

Manon Knockaert (Unamur)

Pauline Lapointe, Darius Štitilis, Andrius Bambalas, Anyssa Fatmi (MRU)

Reviewers (ordered according to beneficiary numbers)

Rayna Stamboliyska (YWH)

Volkmar Lotz (SAP)

Executive Summary

This deliverable focuses on the in-depth analysis of key challenges and promising solution approaches related to a subset of the previous report's aspects. Based on the literature review and a series of interviews with the scholars in the SPARTA Programs, key challenges were identified to lay the foundation for further analysis and meaningful interaction between WP2 and the Programs.

Chapter 2 explains the process of identifying the SPARTA Programs' related legal, societal and ethical challenges and identify the rationale behind choosing particular aspects for further analysis in this Report. A 'standard' car platooning business model alignment with the GDPR compliance and researcher's legal responsibility for disclosing a vulnerability are identified as the legal aspects for further research during the last year of the project.

Chapter 3 focuses on the issues related to GDPR, whereas other Chapters will deal with the questions specific to different SPARTA Programs. During the meetings with the programs' experts, some misinterpretations around the concept of personal data protection were identified and addressed in Chapter 3. The correct understanding of the key definitions of the GDPR is the necessary prerequisite for the successful embedding of the data protection principles while developing a technological solution. The Chapter also reflects on the national security exemption concept established in GDPR, and the preceding Directive. It also reviews the laws and strategies regarding national security that have been enacted by some selected Member States. The research reveals the lack of a clear concept of 'national security' in EU legislation.

Chapter 4 outlines a process that is meant to give practical guidance on how to improve the societal readiness of cybersecurity research projects, helping a working group in its general reflection on what it wishes to achieve, in setting measurable success criteria for the sake of monitoring and evaluation, and in anticipating potential conflicts between actors, their goals and interests that is based upon the concept of Responsible Research and Innovation.

Chapter 5 aims to establish the contents and limitations of Security and Public Order criteria under EU Investment Framework Regulation. The research reveals that the decision on the screening of foreign direct investment based on national security or vital security interests lies within the individual Member States. That includes the determination for on what exactly constitutes security and public order for each member state.

Chapter 6 reviews the EU competence to regulate disinformation since the holistic and systematic approach also require a unified legislative approach toward the phenomena. The use of AVMS Directive and E-commerce directive may be the tools to fight disinformation, however, due to varying concepts of 'illegal content' and national security, embedded in the national law, the protection's effectiveness might differ. This and further analysis will provide a sound basis for the formulation of some of the general guidelines for responsible cybersecurity research and innovation in the next report.

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

Cybersecurity is not a new problem but one that – due to the pervasiveness and complexity of modern computing systems – is becoming more and more critical for the functioning of our society. In recent years security of digital systems has become a matter of strategic importance as impacts diversify and complexity grows higher. In 2007 the cyberattacks on Estonia and the 2010 Stuxnet attacks on Iranian uranium enrichment infrastructure have shown that cyberattacks can have geopolitical implications, and can pose a major risk to the stability of democracies and economies.

After some time of actionism with local and ad-hoc activities Europe has started to address the problem in a coordinated way. SPARTA and the other CCN pilots are part of the European efforts to keep pace in the cyber security arms race with developments from cyber criminals and non-EU countries such as Russia and China (Petratos 2014; Bendiek, Bossong, and Schulze 2017). Cybersecurity measures – as security measures in general – may and actually often do come at the expense of other interests and values, though certain home and security policy makers tend to claim security as superior to other basic rights. This is problematic since in the (cyber)security field there is an inherent imbalance of powers between the involved actors (see Figure 1: The landscape of cybersecurity actors). Those who decide on security measures in politics, industry and law enforcement don't have the same interests and priorities as those who are finally affected by them, namely citizens, companies. Finally, researchers and engineers developing and implementing computer systems in general and cyber security measures in particular may have different ideas and priorities (Spiekermann, Korunovska, and Langheinrich 2019). As an effect possible value conflicts between security and other individual and social values are often solved in favour of security (Knockaert et al. 2020).

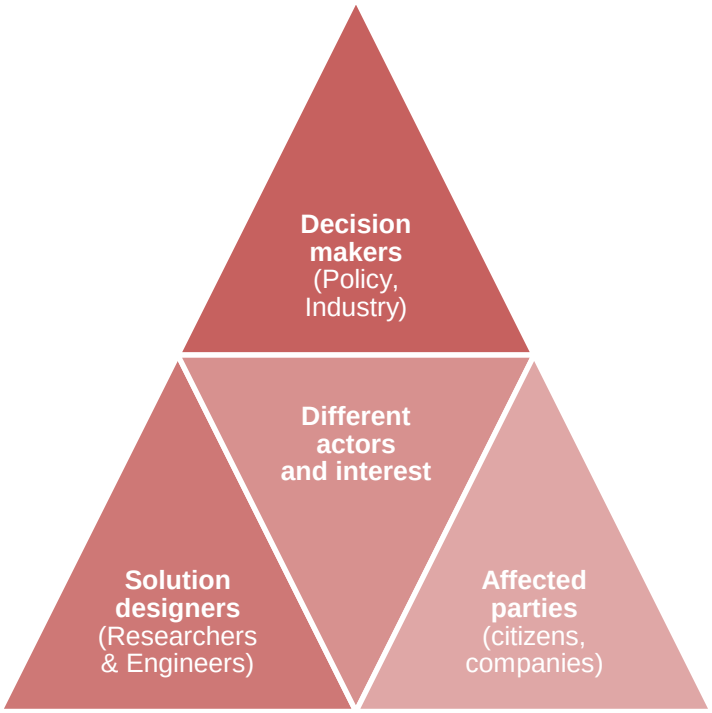


Figure 1: The landscape of cybersecurity actors

To ensure that technologies and practices that tend to infringe with values or even fundamental rights are socially acceptable the interests and impacts have to be made a subject of public deliberation (Burgess et al. 2018). On this basis, technologies and solutions must be designed to reconcile different interests as far as possible. As the following chapters of this deliverable show, the concrete

ethical and legal issues raised by cyber security (research) are numerous and wide-ranging. Against this background, we concluded in an earlier report (Knockaert et al. 2020) that there are no general rules for addressing cyber security related issues beyond very general guidelines, but that each individual case must be considered in its concrete context.

This deliverable focuses on the in-depth analysis of key challenges and promising solution approaches related to a subset of the aspects identified in the previous report. Based on literature review and a series of interviews with the scholars in the Programs, key challenges were identified to lay the foundation for the further analysis and meaningful interaction between WP2 and the Programs. With respect to solution approaches, we pay particular attention to concrete practices that have proven effective in individual cases or in research and innovation areas other than cybersecurity. This analysis will provide us with a sound basis for the formulation of some of the general guidelines for responsible cybersecurity research and innovation in the next report.

Chapter 2 will explain the process of identifying the SPARTA Programs' related legal, societal and ethical challenges and identify the rationale behind choosing particular aspects for further analysis in this Report.

Chapter 3 will focus on fundamental issues related to data protection or the GDPR, whereas other chapters address specific issues of the different SPARTA Programs.

Chapter 4 will outline a process that is meant to give practical guidance on how to improve the societal readiness of cybersecurity research projects, that is intended to help a SPARTA working groups in their reflection on what they aim to achieve, in setting measurable success criteria for the sake of monitoring and evaluation, and in anticipating potential conflicts between actors, their goals and interests that is based upon the concept of *Responsible Research and Innovation* (RRI).

Chapter 5 will define the contents and limitations of the Security and Public Order criteria under EU Investment Framework Regulation based on texts of official EU documents and positions of the EU institutions and practice of the CJEU in cases dealing with limitation of free movement of capital (Article 65 of the TFEU).

Intensified spread of disinformation and manipulative interference requires multidisciplinary and multi-stakeholder approach. EU should develop a holistic, systematic and proactive approach to address the phenomena. Therefore, *Chapter 6* will review the EU competence to regulate disinformation, since the holistic and systematic approach also require a unified legislative approach toward the phenomena.

Chapter 2 Mapping of Specific SPARTA Programs' related problems

Four meetings were held to discuss relevant ELSA with the WPs leaders and scholars researching within the programs. The discussion during the meetings was structured in two parts. The first part was devoted to GDPR issues. A template was provided to ensure structured responses (see Appendix 1). During the second part of the meeting, a non-structured discussion was carried on based on the presentation given by the Program lead on the tasks within the Program and the results already achieved.

The legal, societal and ethical challenges identified by the experts of the WP2 and proposed for consideration by the experts from Programs were grouped (see Appendix 2).

The legal, societal, and ethical issues identified during the discussions with T-SHARK's experts cover aspects different in nature and scope. Some of them are related to the establishment of a national ecosystem for the recognition and analysis of the information disorder that enables full-spectrum cybersecurity awareness. For instance, the legal basis for the possible collection of personal data in open-sources (national security exemption in the context of GDPR), the legality of 'monitoring' process of possible information disorder by the state agents, differentiation between collection and access to personal data. Other questions are related to the effective functioning of the ecosystem and proactive prevention of information disorder. These issues range from the questions related to the general legal framework surrounding the reactive and proactive legal response to disinformation, e.g. absence of commonly agreed and legally approved terminology, the legislative power of the EU to prevent disinformation, lack of a widely agreed legal response to the established influence operations, the screening of foreign investment that might be the source of disinformation, to those directly relevant to the effective functioning of the ecosystem (e.g. the issue of absence of national e-archive, the acceptance of the ecosystem by public).

Possible sharing of personal data was identified as a GDPR specific issue in WP5 (particularly in car platooning). This issue may not be addressed within the main task's scope since it covers mainly technological aspects. However, it was discovered that personal data processing might be an important issue in the business model. Since a tool to analyse GDPR compliance in business processes is created within WP6, the 'standard' car platooning business model can be tested with the tool seeking to evaluate GDPR compliance. This research will be conducted during the last year of the project.

Discussion with the team of WP5 also pinpointed the importance of the question of responsible disclosure of security vulnerabilities (see the policy status in Appendix 5), in particular the issues of the responsibility of a researcher (see the status in Appendix 4). The transposition of the NIS Directive across the Union appeared to be a perfectible tool. Indeed, it is envisioned that a revision of NIS Directive will allow for a "greater level of cybersecurity preparedness" (CEPS, Wavestone and ICF Opening Workshop for DG CONNECT, 2020). Despite its help for a better vision of CVD policy currently implemented, the latest review from DG CONNECT highlights the lack of legal certainty for researchers involved in the discovery of vulnerabilities. This phenomenon is noticeable at the national level (see Appendix 4) but also at the EU level (CEPS, 2020). This could be explained by the legal form and strength chosen to enact the EU Security of Network and Information Systems strategy – a directive instead of a regulation for a better harmonization of practices across the EU (CEPS, 2020).

Hence, the research on CVD within WP2 has also been focusing on the different perspectives to approach the implementation of CVD, particularly the researcher's legal responsibility at stake.

The desk research focused on the new developments since 2018, when the extensive analysis was conducted by CEPS (CEPS, 2018). New legislation was identified in some countries, e.g., Latvia

and Lithuania; some countries have started the discussion on possible regulation of the issue. The approach sustained by most of the EU Member States analysed is a concept of conditional protection of the researcher (see Appendix 4). The pattern is as follows: if researchers, or finders, comply with the guidelines established by the CERT, then they will be able to benefit from protection for their findings. To understand if there is a common standard procedure for reporting and how it influences the establishment of responsibility, it is essential to scrutinise the CERT guidelines and possibly additional legal requirements. This data has been mostly out of reach during the desk research.

The questionnaire established (see Annex 6) will elaborate on the researcher's legal responsibility for disclosure of a vulnerability. The new research will focus on the existing regulation of responsibility of a researcher to compare the different responsibility regime in this regard. By gathering the latest data available since 2018, the questionnaire will allow to draw up an accurate state of play of a researcher's protection across the Union *inter alia* on the following aspects: type of responsibility applicable; legal conditions for responsibility; the scope of the protection granted to the finder or family members.

The questionnaire will also address the procedure of reporting a vulnerability and incentives to encourage the participation to CVD programs. The questionnaire will be sent to different Sparta project partners and stakeholders to gather the latest data related to their national legislations on CVDs. The comparative analysis is expected to be finalised by May 2021.

The key challenges for further investigation were selected jointly and transparently based on a set of predefined criteria: relevance of a solution during the lifetime of the project; relevant of a solution for reception of a particular innovation once it is developed; relevance of a solution for the research. This assessment was mainly performed internally with involvement of experts from different Programs.

This and further analysis during year 3 of the project will present a sound basis for the formulation of some of the general guidelines for responsible cybersecurity research and innovation in T2.3 and also some proposals on policy development of the European Union in cybersecurity area.

Bibliography

CEPS (Lorenzo Pupillo, Afonso Ferreira, Gianluca Varisco), "Software Vulnerability Disclosure in Europe". CEPS. 2018-06-27. Retrieved 2019-10-18. https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/.

CEPS, Wavestone and ICF, Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), June 2020, DG CONNECT.

CEPS, Wavestone and ICF, Workshop: Study to support the review of Directive on Security of Networks and Information Systems, June 2020.

Chapter 3 GDPR related challenges

In Section 3.1 we would like to present the common issues identified among the Programs concerning GDPR compliance during the project's lifetime. During the meetings with the experts working in the Programs, we identified some misinterpretations around the concept of protection of personal data. The correct understanding of the key definitions of the GDPR is the necessary prerequisite for the successful embedding of the data protection principles while developing a technological solution.

Section 3.2 examines exceptions to privacy laws in the context of national security, the category of national security itself and evolving practices. The Section reflects on the concept of the national security exemption established in GDPR and its precedent Directive. We will review the laws and strategies regarding national security that have been enacted by some selected Member States.

3.1 Common issues identified among WPs related to the protection of personal data

In this regard, after determining the purpose(s) of the collection and how to process the personal data, the data controller must determine which personal data are necessary to achieve its purpose. As these are the cornerstone of personal data protection, we focus in this section on the analysis of the concepts of personal data, data anonymization and pseudonymisation, risks of re-identification, and minimisation requirement. As a matter of fact, it is often (and erroneously) believed that the minimisation obligation is limited only to the amount of personal data collected.

After the project, we can expect that the issue of trust and consent of individuals to the technologies developed during the project will be raised. Indeed, while the GDPR provides for several legal bases for the processing of personal data, the use of consent implies that the quality of consent must be verified. For example, consent to the processing of personal data for artificial intelligence technologies or to fight against the phenomenon of disinformation, must be freely given, specific, informed and unambiguous (Recital 32 and Article 7 of the GDPR). That could potentially lead to some questions such as: how to define security requirements in a precise but comprehensive manner to citizens? Should we give more information to the data subject than what is required by the GDPR in order to ensure a transparent processing and to obtain the consent? What information should be given to the data subject to understand the functioning of the system?

3.1.1 Understanding the notion of "personal data"

Through the various discussions with the WPs, it appears that the notion itself of personal data seems ambiguous. The GDPR adopts a broad definition of the notion of personal data, Consequently, the legal definition uses notions that require interpretation on a case-by-case basis. We will therefore try to analyse the definition given by the GDPR in order to understand, in absolute terms, the material scope of application of this regulation and we will give examples taken from the Programs.

The notion of personal data encompasses any type of information. It can cover:

a) *private information*, shared by a restricted group, or even totally confidential (CJEU, C-119/12).

b) *information that has been the subject of dissemination or publication.* In this way, data disseminated in the media, published on a website or shared on social networks can be considered as personal data and therefore do not lose their protection due to their public nature (CJEU, C-131/12).

c) *professional or commercial* information (CJEU, C-301/06; CJEU, C-311/18).

d) both objective, verifiable and questionable information, and subjective information: *opinions, assessments and evaluations of individuals* also fall within the notion of personal data (CJEU, C-434/16).

In Josef Probst v Mr. Nexnet GmbH the applicant failed to pay some charges to Verizon (internet services supplier), his personal data would be exclusively processed for the purpose of that contract and deleted after. However, the Court found out that "externalization" of such data to a Third Party would "affect the level of data protection" granted to the user. The Court held that:

> *The assignee of claims for payment is authorized to process the data on condition that it acts "under the authority" of the service provider and that it processes only traffic data which are necessary for the purpose of recovery of those claims. That provision seeks to ensure that such externalization of debt collection does not affect the level of protection of personal data enjoyed by the user.* (CJEU, C-119/12, p. 18-27).

In *Google Spain and Google* the CJEU held that an Internet search engine is responsible for the processing it carries out of personal data, even when published by Third Parties, as it is responsible for its algorithm. An individual may ask for the withdrawal of his/her personal data from hyperlinks (CJEU, C-131/12, p. 35 to 37).

Ireland v *Parliament and Council* refers to the retention of electronic communication data. The Court, interpreting Directive 2006/24 on the retention of electronic communication data, helding that its provisions are limited to activities of service providers, and not, in any manner, grant and govern access to data or use of it by law enforcement bodies (police or judicial) of Member States (CJEU, C 301/06, p. 90 and 91).

Data Protection Commissioner v. Facebook Ireland Ltd and Schrems covered the issue of transferring data to a Third Country based company from EU soil - the operator must ensure an equivalent protection of personal data (CJEU, C-311/18, p. 101).

In *Novak*, an accountancy student, Peter Nowak, saw his request refused to access a copy of a script of his failed exam. The responsible body in Ireland assumed that the exam transcript did not contain personal data, hence did not fall under the scope of data protection law. Data Protection Commissioner also agreed – the exam script was not personal data. The Irish Supreme Court sought a ruling from the CJEU in this regard, whether the transcript was personal data or not. The Court answered that:

> *the written answers submitted by a candidate at an exam constitute information that is linked to him or her as a person. The content of those answers reflects the extent of the candidate's knowledge and competences in a given field, and in some cases, his intellect, thought processes, and judgment.* (CJEU, C-434/16, p. 34, 43)

In addition, a link must be established between the data and a living natural person. Indeed, the data must "concern" the person in question (Article 29 Working Party, 2007; C. de Terwangne, 2018, p. 59; C. de Terwangne et al., 2019, p. 15). According to the CJEU: "This last condition is met when, by virtue of its content, purpose or effect, the information is linked to a specific person" (CJEU, C434/16, p. 35; C. de Terwangne et al., 2019, p. 15).

For example, in CAPE program, the focus is on the security of the meassage exchanged betwen the cars in platoon. As an example, it could be interesting to keep in mind that even if the vehicle unique identifier is protected by a cryptography technology, it is still a personal data, because it allows (indirectly) the identification of the car owner/driver.

Another example could be found in T-SHARK and the concrete scenario of fake news. The IP address, the name of the social media user and his/her picture, and religious and political beliefs should be considered as personal data.

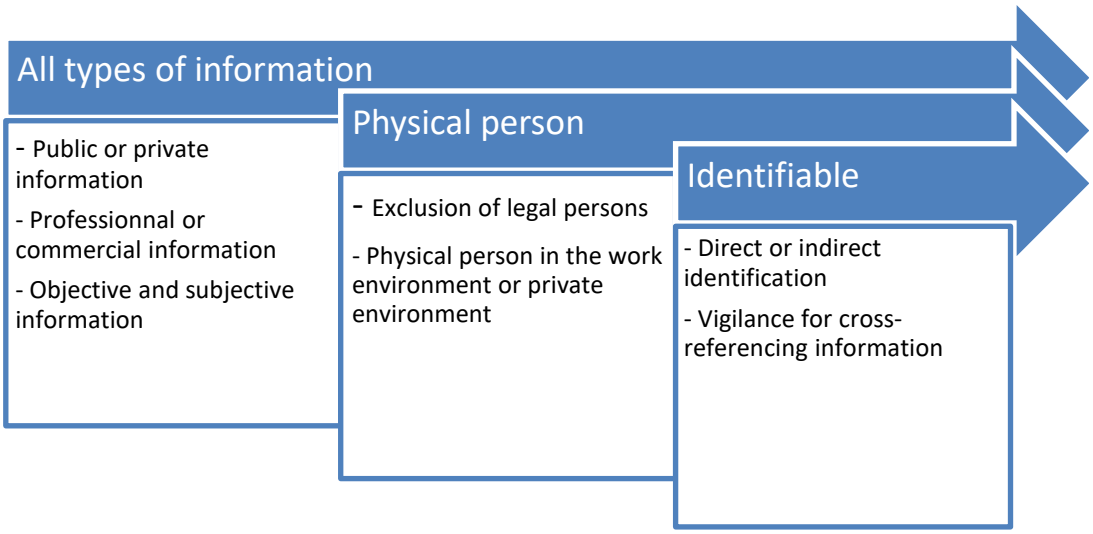


Figure 2: The link between data and a physical person

3.1.2 Anonymisation/pseudonymisation

The interest of the distinction is that anonymised data is not in the scope of the GDPR, as it is no longer personal data. On the contrary, pseudonymised data is still considered as personal data, which implies the application of the GDPR with some particularities of application (E.g. see Article 11).

The GDPR does not provide any definition of "anonymous data". A negative definition can be found in the Directive 2019/1024 on open data and the re-use of public sector information. It precises that the notion of anonymisation should be understood as:

> *"the process of changing documents into anonymous documents which do not relate to an identified or identifiable natural person, or the process of rendering personal data anonymous in such a manner that the data subject is not or no longer identifiable"* (article 2.7 of the Directive (EU) 2019/1024).

Additionally, the previous legislation for the protection of personal data, the Directive 95/46/EC (1995) indicated that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person" (Recital 26). This is also reflected in Recital 26 and in Article 4.1 of the GDPR.

The former Article 29 Working Group (now replaced by the European Data Protection Board) called, before the entry into force of the GDPR, for a distinction between anonymisation and other techniques to mitigate risks of re-identification of the data subjects (Article 29 Working Party , 2013, p. 13).

Most recently, a definition could be found in the Directive (EU) 2019/1024 on open data and the re-use of public sector information (ENISA, 2015; ENISA, 2019; Commission Nationale de l'Informatique et des Libertés, 2020). According to Article 2.7 of the Directive, anonymisation means:

the process of changing documents into anonymous documents which do not relate to an identified or identifiable natural person, or the process of rendering personal data anonymous in such a manner that the data subject is not or no longer identifiable.

Previously, the former Article 29 Working Party defined anonymisation as the:

results from processing personal data in order to irreversibly prevent identification. In doing so, several elements should be taken into account by data controllers, having regard to all the means "likely reasonably" to be used for identification (either by the controller or by any third party) (Article 29 Data Protection Working Party, 2014, p. 3).

Furthermore, it states that the technique of anonymisation should be akin to data erasure, i.e. it should make it impossible to process personal data (Article 29 Data Protection Working Party, 2014, p. 6).

Consequently, in order to be able to declare that he/she is working with anonymous data, the data controller must be certain that it is no longer possible, with reasonable means, to identify individuals, even by cross-referencing data. Big data makes it increasingly complex to qualify the data as anonymous (ENISA, 2015)

Very often, the notion of anonymisation is confused with the notion of pseudonymisation. According to Article 4.5 of the GDPR, pseudonymisation means:

> *the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*

Figure 3: Anonymisation

Figure 4: Pseudonymisation

In conclusion, the great difference between these two methods is that complete anonymisation no longer makes it possible to identify the person concerned with reasonable means (Recital 94 of the GDPR). Pseudonymised data, on the other hand, are considered to be identifying data. In fact, it is sufficient to have the additional initial information (e.g. a key to decipher an encrypted file) to identify the person.

For example, in CAPE, each car has its own unique identifier. According to what information are contained into the messages exchanged between cars in a platoon, it could be useful to identify if the data exchanged are 1) personal data or not and 2) if it is pseudonymised or anonymised data. The same question could be raised in the processing of personal data in intelligent infrastructures (HAII-T Program).

3.1.2.1 How to evaluate an anonymisation solution?

If the aim is to avoid the possible identification and individualisation of the data subject, it should be remembered that the legislation framing the protection of personal data does not give any indication as to the technology to be used to achieve the anonymisation of personal data. Indeed, the GDPR aims to be technologically neutral.

In order to assess the quality of the anonymisation technology chosen, several criteria must be taken into consideration (Article 29 Data Protection Working Party, 2014, p. 3):

- Is it still possible to single out an individual?
- Is it still possible to link records relating to an individual?
- Can information be inferred concerning an individual?

This analysis requires a case-by-case assessment based on the state of the art in anonymisation technologies and on the reasonable means available to third parties to achieve the identification of an individual (Commission Nationale de l'Informatique et des Libertés, 2020).

In the Opinion 05/2014, the Article 29 Data Protection Working Party provided an opinion on the Anonymisation Techniques. The aim of this opinion was to analyse the effectiveness and limits of the current anonymisation techniques against the changes brought by the adoption of the GDPR.

Indeed, according to Recital 26 of the GDPR, personal data that have been pseudonymised and that still may be attributed to a physical person via the use of additional information, should still be considered as data concerning an identifiable person (Recital 26). Therefore, the Working Party had to reflect on the different methods on anonymisation techniques that can provide privacy guarantees, but that can also be used to generate "efficient anonymisation processes".

The Working Party highlighted the need, for an "optimal solution", to process on a casuistic approach (Article 29 Data Protection Working Party, 05/2014). Indeed, a case-by-case basis, combining different techniques, may be the most suitable way to comply with privacy guarantees. Finally, Opinion 05/2014 emphasises that pseudonymisation is not a method of anonymisation – it is only a reduction of the "linkability of a dataset" with the original identity of a data subject. Hence, anonymisation is not a "one-off" exercise, but rather an evolving area where reassessment shall be made regularly by data controllers (Article 29 Data Protection Working Party, 05/2014).

3.1.2.2 Three criteria for evaluating the pseudonymised personal data

In contrast to anonymisation, pseudonymised personal data makes possible to re-identify the data subject. This imposes to keep the additional information necessary to identify the data subjects separately from the coded/pseudonymised data.

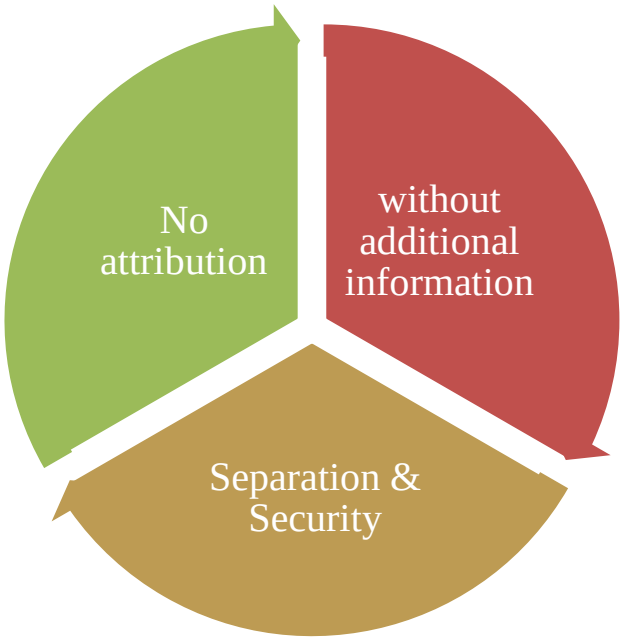


Figure 5: Criteria for evaluating the pseudonymised personal data

In order to ensure an effective pseudonymisation, three pillars are necessary. Firstly, no attribution of data collected implies the inability to link information to an identified or identifiable individual (Article 4(3b) of the GDPR). Second, pseudonymisation is defined as in compliance with GDPR when, the processing of personal data is done "without the use of additional information" (Article 4(3b) of the GDPR). However, and finally, when done otherwise, the collection of additional information must be "kept separately" and secured by technical and organizational measures to ensure a secure and collection of personal data in compliance with GDPR (Article 4(3b) of the GDPR).

3.1.3 Re-identification risks

The risk of re-identification is an essential component of the concept of anonymised data. Indeed, before being able to consider working with anonymised data (and therefore data for which the GDPR is not applicable), the controller must ensure that re-identification of the data subject is no longer possible by reasonable means (Recital 26 of the GDPR).

The data controller must consider the state of the art to check what are the reasonable means available to any (third) party trying to reverse the anonymisation of personal data. As explained by the Article 29 Working Party,

> *the means likely reasonably to be used to determine whether a person is identifiable" are those to be used "by the controller or by any other person". Thus, it is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data. Only if the data controller would aggregate the data to a level where the individual events are no longer identifiable, the resulting dataset can be qualified as anonymous (…) An effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset. Generally speaking, therefore, removing directly identifying elements in itself is not enough to ensure that identification of the data*

> *subject is no longer possible. It will often be necessary to take additional measures to prevent identification, once again depending on the context and purposes of the processing for which the anonymised data are intended* (Article 29 Data Protection Working Party, 05/2014, p. 9).

For example, this issue could be of particular relevance in the case of intelligent infrastructures and internet of things. Indeed, intelligent infrastructures and the internet of things are characterised by a significant amount of data collection and processing, some of which is personal data. It is important for the data controller to identify the risks of re-identification of data subjects before being able to declare that its technology is using anonymous data.

Criteria to be considered to avoid re-identification (Article 29 Data Protection Working Party, 6/2013) are important in this context**.** In the discussion on personal data and access to public sector information, the Article 29 Working Party established the criteria for assessing the risk of re-identification of a data subject and thus evaluating the degree of anonymisation or pseudonymisation of a data item**.** Meeting of three criteria makes it possible to reach the threshold required by the legislation governing the protection of personal data in order to qualify the data as anonymous. These are:

Criterion 1: What other data are available? There is a possible risk of re-identification if the data to be published could be linked to other datasets:

- Either by cross-referencing internal data (the cross-referencing of two data sets which, separately, are anonymised may allow indirect identification through cross-referencing and fall within the scope of the GDPR); or
- Either by cross-referencing external data either for the general public or for other persons or organisations

Criterion 2: The likelihood of a re-identification attempts by the candidate re-user or by a third party (some types of data will be more interesting for potential intruders than others);

Criterion 3: The likelihood that re-identification by the candidate re-user or by a third person, if attempted, would be successful, given the effectiveness of the proposed anonymisation techniques[1]. As a good practice, it is recommended that a pentest be carried out. On this last aspect, the Article 29 Working Party states that:

> *This consists of attempting to re-identify individuals from the datasets that are planned to be released. The first stage of a re-identification testing process should be to take stock of the datasets that the public sector body has published or intends to publish. The next stage should be to try to determine what other data - personal data or not - are available that could be linked to the data to result in reidentification. Targeted 'penetration tests', in particular, should help assess what are the risks of jigsaw identification, i.e. piecing different bits of information together to create a more complete picture of someone. Of course, re-identification testing should not be considered as a panacea and should not lead to a false sense of security. First, the testing could be difficult to perform since it often requires significant technical expertise and adequate tools, as well as awareness of what other data may be available. Second, data controllers must also be aware that the risk of re-identification can change over time* (Article 29 Data Protection Working Party, 06/2013, p. 17).

[1] One example of anonymisation technique could be the differential privacy. The data controller must choose the best anonymisation or pseudonymisation technique with regard to the costs, the state of the art, the nature of the personal data, the amount of personal data and the risks of its processing activities. Each technique used must be analysed with regard to the risk of re-identification.

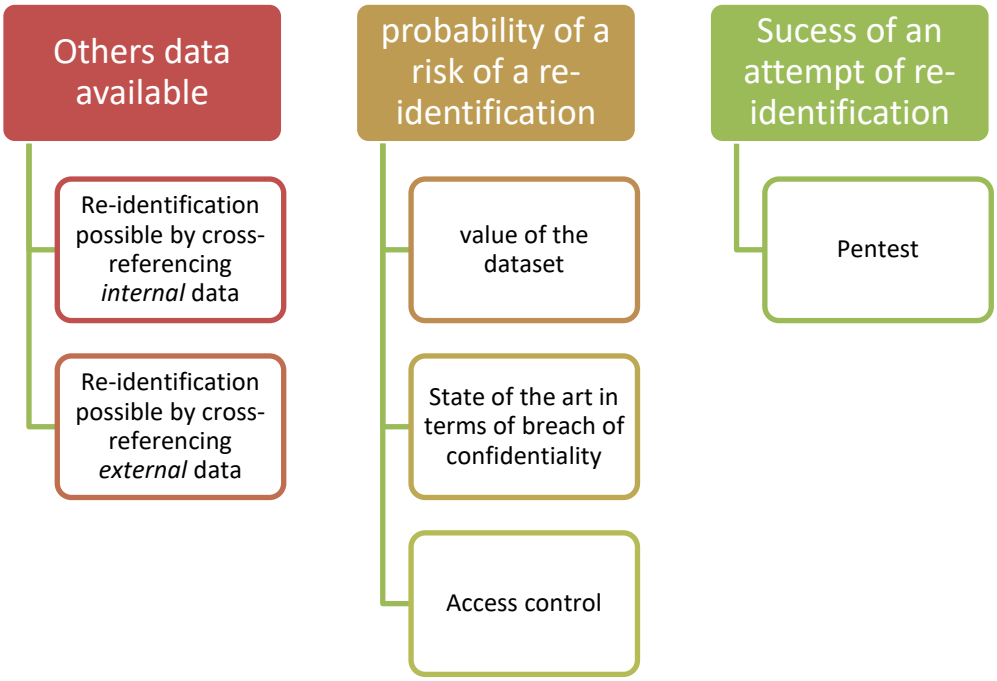


Figure 6: Criteria to be considered to avoid re-identification

3.1.4 Minimisation principle

Article 5 of the GDPR states that the personal data collected and processed has to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This requirement derives from Article 8 of ECHR stating that everyone has the right to be respect for his private and family life. The limitation of the collection of personal data (pseudonomised or not) to data that is strictly necessary for the fulfilment of the purpose is a fundamental obligation for the respect of the privacy of individuals.

Implementation of the minimisation principle may be challenging. The data controller must remain proportional in the data collected and the processing carried out. Thus, the criteria to be taken into account are: the amount of personal data collected; the storage period; accesssibility to the personal data.

The amount of personal data collected. The guidelines from the European Data Protection Board state that this criterion refers to both the quantity and quality of the data collected:

> *"Controllers must consider both the volume of personal data, as well as the types, categories and level of detail of personal data required for the processing purposes. Their design choices should take into account the increased risks to the principles of security, data minimisation and storage limitation when collecting large amounts of detailed personal data, and compare that against the reduced risks of collecting less finely detailed information about data subjects"*
> (EDPB, 2019, p. 11-12)

The storage period. The GDPR states that personal data may not be kept for longer than necessary to fulfil the purpose(s) pursued by the data controller. The data controller must therefore determine the purpose of the processing of personal data and, depending on it, define the necessary

conservation period[2]. Particularly in the context of IoT, the period of conservation could be different according to the various stakeholders (e.g. creator of the algorithm, creator of the sensors, vehicle manufacturers). In this regard, the Article 29 Working Party indicated that:

> *This necessity test must be carried out by each and every stakeholder in the provision of a specific service on the IoT, as the purposes of their respective processing can in fact be different. For instance, personal data communicated by a user when he subscribes to a specific service on the IoT should be deleted as soon as the user puts an end to his subscription. Similarly, information deleted by the user in his account should not be retained. When a user does not use the service or application for a defined period of time, the user profile should be set as inactive. After another period of time the data should be deleted* (Art. 29 Working Party, 8/2014, p. 17)

Accessibility to the personal data. According to the European Data Protection Board,

the controller must limit who can have access to personal data based on an assessment of necessity, and also make sure that personal data is in fact accessible to those who need it when necessary, for example in critical situations. Access controls must be observed for the whole data flow during the processing. Article 25(2) further states that personal data shall not be made accessible, without the individual's intervention, to an indefinite number of natural persons. The controller must by default limit accessibility and consult with the data subject before publishing or otherwise making available personal data about the data subject to an indefinite number of natural persons (EDPB, 2019, p. 12).

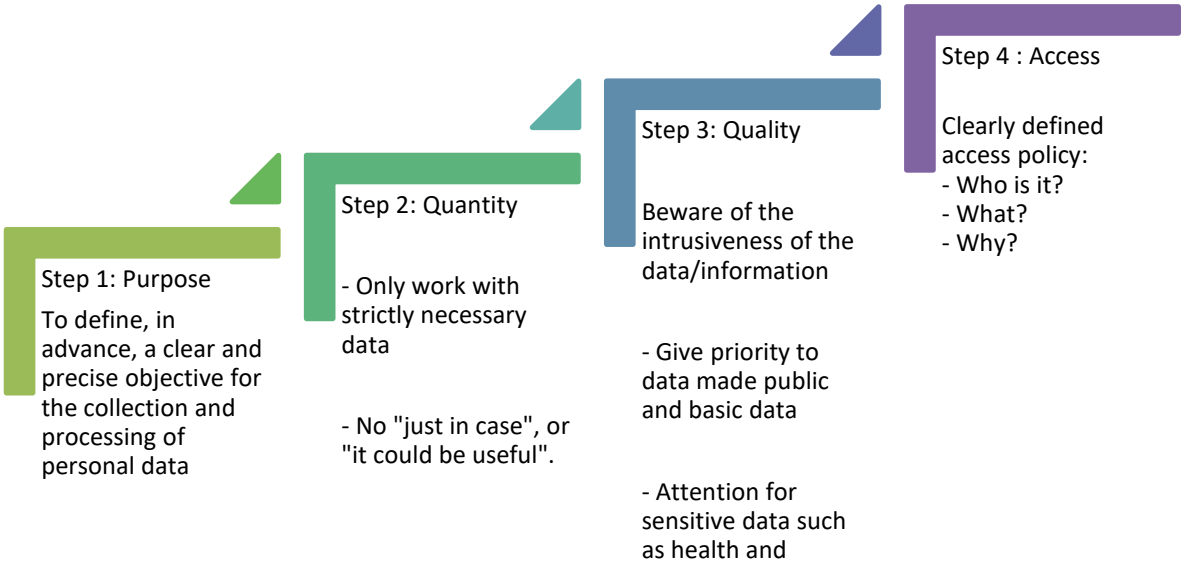


Figure 7: Implementation of the minimisation principle: criteria

3.2 National Security Exemption in GDPR

Evolving cyber-threats varying in scope, scale, duration, intensity, complexity, sophistication and impact, are getting increasingly common and demand a mobilization of the full range of respective tools and instruments, as well as a joint response. Some of the threats may be directed against the values that make up the concept of national security. This is emphasized in the reports of the security services of various states. Various tools can be used to combat cyber threats to national security,

[2] When the processing of personal data is based on compliance with a legal obligation, the retention period should be determined by the law.

one of which is threat prediction, which can provide timely warning of emerging threats. This may be the way to move from a reactive model to a proactive response model as well.

For the prediction of cyber threats, related analysis requires large amounts of information, which may include personal information that is protected by privacy laws. However, different rules may apply in cases of national security. It is therefore important to examine exceptions to privacy laws in the context of national security, the category of national security itself and evolving practices. This question is of particular relevance to T-SHARK program, which advocates for the extension of cybersecurity threat intelligence and its enrichment with the related external information and information from other security domains, as well general context information, that allows to perform Full Spectrum Analysis.

3.2.1 Personal data protection in the context of national security

The processing of personal data for national security purposes has not been in focus for many years. But things changed in 2013. Edward Snowden, a former contractor for the CIA, left the US in late May after leaking to the media details of extensive internet and phone surveillance by American intelligence. The scandal broke in early June 2013 when the Guardian newspaper reported that the US National Security Agency (NSA) was collecting the telephone records of tens of millions of Americans. The paper published the secret court order directing telecommunications company Verizon to hand over all its telephone data to the NSA on an "ongoing daily basis". That report was followed by revelations in both the Washington Post and Guardian that the NSA tapped directly into the servers of nine internet firms, including Facebook, Google, Microsoft and Yahoo, to track online communication in a surveillance program known as Prism (BBC, 2014).

After this scandal the world has changed. Discussions have begun on the activities of law enforcement agencies in collecting personal data and the validity of these activities, the relationship with the right to privacy.

Not only that, the scandal began to spread. Britain's electronic eavesdropping agency GCHQ was also accused of gathering information on the online companies via Prism. The GCHQ scandal widened on 21 June when the Guardian reported that the UK spy agency was tapping fibre-optic cables that carry global communications and sharing vast amounts of data with the NSA, its US counterpart (BBC, 2014).

These events revealed a series of cases of mass surveillance of individuals. Not only has this sparked a debate about the legitimacy of such surveillance, but it has done immense damage to public confidence in their state, in their national security institutions.

3.2.2 National security and EU personal data protection law

Before going into the specifics of EU legislation, it is necessary to reflect on the concept of the national security exemption imposed by Article 4(2) of the TEU. This article states that

> *the Union shall respect the equality of Member States (...) as well as their national identities (...) It shall respect their essential state functions, including (...) safeguarding national security. In particular, national security remains the sole responsibility of each Member State.*

Therefore, EU law, including the Charter of Fundamental Rights of the European Union (hereinafter - the Charter), shall not apply to matters regarding the national security of Member States. This is an important exemption to the applicability of EU law (Article 29 Working Party, WP 228, p. 22).

Since 1995 there were exceptions to national security in EU law governing the protection of personal data. In the preamble of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on

the free movement of such data (hereinafter - General data protection directive or Directive[3]) was specified that

> *(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law.*

Thus, the Directive[4] already stated that the national security is out of the scope of the EU law.

Recital 43 of the preamble to the Directive states that in the case of national security, as in the other cases mentioned, rights of access and information and certain obligations of the controller may be restricted. Moreover, the exemptions and restrictions are validated in Article 13 of the Directive:

> *Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes necessary measures to safeguard: (a) national security <…>.*

The provisions of this Article presuppose that, in the case of national security, certain rights and obligations may be restricted. This does not mean that the protection of personal data does not apply at all in the case of national security - in the case of national security, appropriate restrictions on rights and obligations may be imposed.

It is important to mention that, in addition to the national security exception, the Directive also provides for other cases where restrictions on the protection of personal data apply. In total, the Directive contains 6 such cases in addition to the national security exception: (a) defence; (b) public security; (c) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (d) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (f) the protection of the data subject or of the rights and freedoms of others.

Thus, even without analyzing the category of national security, one sees that this is not the case of defence, public security, the prevention, investigation, detection and prosecution of criminal offences. National security is a category separate from these mentioned categories. The concepts of “national security”, “state security”, “public security” and defense all need to be distinguished from one another (Article 29 Working Party, WP 228, p. 23). However, there are no clear criteria to separate the concepts.

The term of national security is not developed in the Directive itself. However, Article 29 Working Party (Article 29 Working Party, 2020) tried to interpret the term in its opinions, which are considered as soft law[5]. In the *Working Document on surveillance of electronic communications for intelligence and national security purposes* (p. 2) the Working Party advocates on national security concept in the context of electronic communications control. The Working Party indicates:

[3] This Directive is currently not in force and was replaced by GDPR in 2018.

[4] In order to assess the current GDPR provisions on national security in a more comprehensive way, a brief reference to the provisions of the former Directive should be made.

[5] OECD defines soft-law as co-operation based on instruments that are not legally binding, or whose binding force is somewhat "weaker" than that of traditional law, such as codes of conduct, guidelines, roadmaps, peer reviews (OECD, n.a.)

In absence of a clear definition of 'national security', the Working Party has examined how this notion should be interpreted, especially since the thin line between law enforcement and national security sometimes seems to fade. In any case, national security needs to be distinguished from the security of the European Union, but also from State security, public security and defence. All of these notions are referred to separately in the EU treaties and underlying legislation, although they are inextricably linked. Whether or not something should be defined as falling under the national security exemption therefore cannot only be explained by strictly legal arguments. What can be said is that, whereas activities by intelligence and security services are generally accepted as falling under the national security exemption, this is not always the case when general law enforcement authorities fulfil similar tasks.

In 2018 the Directive has been replaced by GDPR. The preamble (Recital 16) to the regulation on application in the case of national security is very clear:

This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security.

As in the Directive, in Article 23 of GDPR national security is singled out among the other exceptions to the application. Although the number of exceptions has increased slightly, national security has remained one of the restrictions.

It is important to mention that this Article sets out specific conditions in the event of an restriction:

Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard.

Thus, restrictions may be imposed by national law. In this case, it is very important to define the category of national security itself and to determine which cases fall into this category and what it covers.

Thus, the legal regulation in the GDPR concerning the national security exception is essentially similar to that in the previous Directive. It should be mentioned, that the opinion of Article 29 Working Party raised the idea of applying a national security exception:

„When assessing the applicability of the national security exemption, it should also be taken into account whether it is a general exemption that applies, as the one laid down in the Treaties and Article 3(2) Directive 95/46/EC, or whether it is part of a provision excluding certain safeguards for reasons of national security. The latter is for example the case when allowing Member States to impose limits to the right of access of a data subject for reasons of national security, as provided by article 13(1)a Directive 95/46/EC" (Article 29 Working Party, WP 228, p. 25).

The Directive is no longer in force, but the GDPR imposes similar restrictions. However, these guidelines were not endorsed (EDPB, n/a)[6] during its first plenary meeting of the EDPB and can no longer be referred as soft law.

It can be stated that national security, despite European integration, explicitly remained the responsibility of member states (Žalnieriūtė, 2020), although there are other trends in European court cases, which are described below.

In summary, despite some attempts to interpret the concept of national security in soft EU law, there is no clear definition of what is to be understood as 'national security' in EU legislation. So far, such criteria of national security have become clear: activities by intelligence and security services are generally accepted as falling under the national security exemption; also, national security cannot be considered as defence, state security, public security, the prevention, investigation, detection and prosecution of criminal offences, etc. And there are no clear criteria to distinguish between these categories.

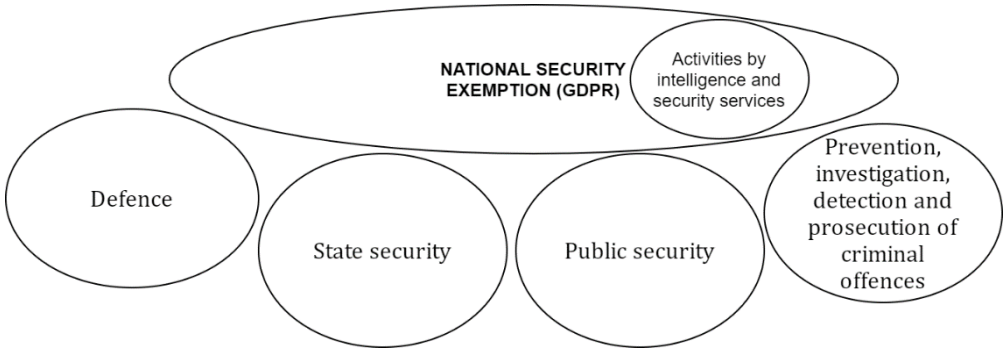


Figure 8: National security exemption

3.2.3 National security concept in national legislation of EU countries

Although non-European practices will not be addressed in this research, it should be noted that the 9/11 attacks in 2001 brought the US government's fear of terrorism to a boiling point, leading to the Patriot Act - a new national security law which expanded the powers of US law-enforcement departments in monitoring citizens' information and in detaining and expelling expatriates suspected of having links to terrorism (Global Times, 2020). The fact that the US has so many security laws shows that they attach great importance to national security legislation and cannot tolerate threats to any aspect of national security.

Similar to the US, European governments also attach great importance to establishing and improving their national security legislation. Plagued by separatist forces, Spain issued its National Security Strategy in 2013 and enacted a National Security Law in 2015 (Ley 36/2015, Art. 3). For a variety of reasons, some other states did the same. In this section, we will review the laws and strategies regarding national security that have been passed by EU Member States.

The Spanish National Security Law provides the following definition of national security:

> *For the purposes of this law, National Security shall be understood as the action of the State aimed at protecting the freedom, rights and well-being of citizens, guaranteeing the defense of Spain and its constitutional principles and values, as well as to contribute together with our partners and allies to international security in compliance with the Commitments assumed.* (Ley 36/2015, Art. 3)

[6] During its first plenary meeting the European Data Protection Board endorsed the GDPR related WP29 Guidelines

As we can see, the definition of national security, while indicating the basic criteria, is sufficiently abstract in nature.

Poland has not adopted a separate national security law, but a new National security strategy (2020) is in place in Poland. According to the strategy, national interests in the field of national security include:

1) Guarding independence, territorial integrity, sovereignty and security of the state and its citizens.
2) Shaping international order, based on solidarity and respect for international law, which guarantees safe and secure development of Poland.
3) Strengthening national identity and guarding national heritage.
4) Ensuring conditions for sustainable and balanced social and economic development and environment protection (p. 11).

There is no direct definition of national security in Lithuania, but features of national security can be distinguished from the provisions of existing legal acts.

According to the Law on the Basics of National Security (1996),

> *the goal of the national security policy is to develop and strengthen democracy, ensure the safe status of the Nation and the internal and external security of the state, deter every potential attacker, defend the independence of the Lithuanian state, territorial integrity and the constitutional order* (Art. 1(2)).

This law also specifies the main objects of national security, which are as follows:

- human and civil rights, freedoms and personal security;
- the values cherished by the nation, its rights and the conditions of free development;
- state independence;
- constitutional order;
- integrity of the state territory;
- environment and cultural heritage;
- public health (chapter 2, sub-chapter 1).

We see that the categories given relate to national security, although listed exhaustively, are of a rather general nature. The practical application may raise a number of questions as to what specific cases fall within national security.

Meanwhile, in Latvian National Security law (2002) the concept of national security is presented: „National security is a state, attained as a result of joint, purposeful measures implemented by the State and society, in which the independence of the State, its constitutional structure and territorial integrity, the prospect of free development of society, welfare and stability are guaranteed" (Section 1 (1)).

According to the National Security Law of Latvia, the tasks of the national security system are the following (Section 3(2)):

> *1. to forecast in a timely manner and prevent internal and external danger to the State, to guarantee State defence, public safety and democratic development of society;*
>
> *2. to draw up a joint, systemic policy of national security for the institutions implementing State authority and administration, and to implement, in a co-*

ordinated and purposeful manner, the legal, economic, social, military, security and other measures determined by the State, at all levels of State administration;

3. to ensure effective management to overcome situations dangerous to the State.

The law lists in detail how the exceptions[7] related to national security apply, but the application of the exceptions related to the protection of personal data is not regulated.

In general, where a definition of national security has been provided in the law, the term tends to be broadly defined to encompass any threats to the independence, sovereignty, or territorial integrity of the nation, as well as to its internal safety or constitutional order (Jacobsen, 2013, p. 8).

Moreover, the European Commission of Human Rights considered that it could not be comprehensively defined, thus giving it a degree of elasticity and hence flexibility, which is reflected by the margin of appreciation which states have in this sphere (ECtHR, 2013, p. 4).

Thus, the concept of national security is regulated in individual states, but it is not very specific. Attempts to define it very specifically seem to go unnoticed. At present there is no uniform national definition in the laws of the EU countries.

3.2.4 National security in CJEU and Jurisprudence

The only institution able to provide more legal certainty on what should and what should not be regarded as falling under the national security exemption is the CJEU. Only the Court can further define the scope of Union law and – subsequently – the applicability of the Charter (Article 29 Working Party, WP 228, p. 24).

Underlying the CJEU decision in *Schrems I and Schrems II* that invalidated the EU-U.S. Safe Harbor agreement and in this most recent case, invalidated the EU-U.S. Privacy Shield, is a disconnect between the GDPR's international impacts, and its domestic application to Member States' national security agencies. In both *Schrems* cases, the issue was U.S. government access to personal data for national security purposes and the rights of EU citizens in the U.S. to judicial review and redress. In both cases the CJEU found that the U.S. fell short in that the U.S. was not according EU personal data the protection and rights of redress available in the EU. When it comes to access to data for national security purposes, under EU law, including GDPR, any limitation on EU rights to privacy must be "necessary and proportionate". At the same time, national security is the sole responsibility of member states (Meltzer, 2020).

In one of the last cases (CJEU, C-511/18, C-512/18 and C-520/18) on the 6th of October of 2020, the CJEU handed down Grand Chamber's judgements determining that the ePrivacy Directive does not allow for EU Member States to adopt legislation intended to restrict the scope of its confidentiality obligations unless they comply with the general principles of EU law, particularly the principle of proportionality, as well as fundamental rights under the Charter (Hunton Andrews Kurth, 2020). The case concerned the processing of personal data in the context of national security. Of course, the case concerns individual circumstances, but in this case national security is specifically linked to the prevention of terrorism (CJEU, C-511/18, C-512/18 and C-520/18, p. 179-182).

After this case, opinions were heard that the CJEU has become an important actor in regulating national security and intelligence activities in EU member states. The emergence of an EU actor capable of seriously influencing national powers of surveillance is relatively new (Žalnieriūtė, 2020).

[7] Restrictions on Commercial Companies of Significance to National Security (Chapter VI of the Law)

However, in addition to the CJEU, ECtHR also ruled on national security issues. In the *Rotaru v. Romania* case[8], the ECtHR (ECtHR, 2000, paras. 53-63) ruled similarly that the data collected has to be relevant to the national security purpose pursued and that, even in a national security context, the law should define the kind of information that may be recorded, the categories of people against whom surveillance measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed and lay down limits on the age of information held or the length of time for which it may be kept. It should also contain explicit and detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information thus obtained (Article 29 Working Party, WP 228, p. 25).

Neither the relevant provisions of EU law, nor the CJEUs / ECtHR case law offers a clear definition of what 'national security' is. Moreover, the EU and its Member States use various rather similar notions related to security without defining them: internal security, national security, State security, public security and defence should all be distinguished (Article 29 Working Party, WP 228, p. 24). It is considered that any cyber threat analysis and prediction system should comply with national requirements related to the protection of national security. And in order to use such kind of systems acting also outside one EU country, greater harmonization of national security concepts should be initiated.

Bibliography

Amanda L. Jacobsen (2013) *National Security and the Right to Information in Europe*, 2013, https://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe

Article 29 Working Party (2014), Working Document on surveillance of electronic communications for intelligence and national security purposes. WP 228, 5 December 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf

Article 29 Working Party. Glossary. https://uk.practicallaw.thomsonreuters.com/1-508-0312?transitionType=Default&contextData=(sc.Default)&firstPage=true

BBC news, "Edward Snowden: Leaks that exposed US spy programmed", January 17, 2014, https://www.bbc.com/news/world-us-canada-23123964

C. de Terwangne (2018), "Définitions clés et champ d'application du RGPD », *in Le règlement général sur la protection des données RGPD/GDPR*, C. de Terwangne and K. Rosier, Brussels, Larcier, 2018

C. de Terwangne, E. Degrave, A. Delforge and L. Gérard (2019), "La protection des données à caractère personnel en Belgique : manuel de base", Brussels, Politeia, 2019

Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority), https://www.cnil.fr/en/sheet-ndeg1-identify-personal-data.

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, Official Journal C 326, 26/10/2012 P. 0001 – 0390, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT

Directive (EC) 95/46 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995, *O.J.*, L 281/31.

[8] Rotaru v. Romania judgment, 4 May 2000, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586#{%22itemid%22:[%22001-58586%22]}, paras. 53-63.

Directive (EU) 2019/1024 of the European Parliament and of the Council on open data and the re-use of public sector information (recast), 20 June 2019, *O.J.*, L 172/56.

ECtHR (2013), Research division, "National security and European case-law", 2013, https://rm.coe.int/168067d214.

EDPB, "GDPR: Guidelines, Recommendations, Best Practices", https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

ENISA (2015), "Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics", December 2015

ENISA (2019), "Pseudonymisation techniques and best practices – Recommendations on shaping technology according to data protection and privacy provisions", November 2019

Global Times (2020), "National security laws are a common global practice: observers", 2020, https://www.globaltimes.cn/content/1189528.shtml

Hunton Andrews Kurth (2020), "CJEU Restricts Indiscriminate Access to Electronic Communications for National Security Purposes", October 12, 2020, https://www.huntonprivacyblog.com/2020/10/12/cjeu-restricts-indiscriminate-access-to-electronic-communications-for-national-security-purposes/

Joshua P. Meltzer (2020), "The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security", August 5, 2020, https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10389-consolidado.pdf

Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas VIII-49 (1996), https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/asr

National Security Law of Latvia, https://likumi.lv/ta/en/en/id/14011-national-security-law

National Security Strategy Of The Republic Of Poland (2020) https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

OECD, https://www.oecd.org/gov/regulatory-policy/irc10.htm

Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88

Žalnieriūtė M (2020). The Future of Data Retention Regimes and National Security in the EU after the Quadrature Du Net and Privacy International Judgments. American Society of International law, Volume 24, Issue 28, November 5, 2020, https://www.asil.org/insights/volume/24/issue/28/future-data-retention-regimes-and-national-security-eu-after-quadrature

ECtHR (2000), judgment of 4 May 2000, *Rotaru v. Romania*, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586#{%22itemid%22:[%22001-58586%22]}

Article 29 Working Party (2007), Opinion 4/2007 on the concept of personal data, 20 June 2007, WP 136

CJEU (2009), judgment of 10 February 2009, *Ireland* v *Parliament and Council*, C-301/06, EU:C:2009:68

CJEU (2012), judgment of 22 November 2012, *Josef Probst v Mr. Nexnet GmbH*, C-119/12, ECLI:EU:C:2012:748

Article 29 Working Party, Opinion 06/2013 on open data and public sector information reuse, 5 June 2013, WP207, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf

Article 29 Working Party (2013), Opinion 6/2013 on open data and public sector information reuse, 5 June 2013, WP207

Article 29 Working Party (2014), Opinion 5/2014 on Anonymisation Techniques, 0829/14/EN WP216, 10 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

CJEU (2014), judgment of 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317

Article 29 Working Party (2014), Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16.09.2014, WP 223

CJEU (2017), judgment of 20 December 2017, *Novak*, C-434/16, ECLI:EU:C:2017:994

EDPB (2019), Guidelines 4/2019 on Article 25 Data Protection by Design and By Default, 13 November 2019

CJEU (2020), judgment of 16 July 2020, *Data Protection Commissioner v. Facebook Ireland Ltd and Schrems*, C-311/18, ECLI:EU:C:2020:559

CJEU (2020), judgment of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18. http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=7638753

Chapter 4 Responsible Cybersecurity Research and Innovation

4.1 Introduction

This chapter outlines a process that is meant to give practical guidance on how to mature the societal readiness of cybersecurity research projects, helping a working group in its general reflection on what it wishes to achieve, in setting measurable success criteria for the sake of monitoring and evaluation, and in anticipating potential conflicts between actors, their goals and interests that is based upon the concept of RRI.

Section 3.2 presents the general ideas behind RRI, developed some ten years ago and adopted by policy makers, in particular the European Commission, as an appropriate basis for technology development in ICT and security technologies fields. Section 3.3. will then explain how the ideas of RRI can be operationalised by adapting the popular concept of technology readiness in terms to social readiness. Section 3.4. will then then proposes a (generic) process that can be used as part of the technical development process to ensure and incrementally improve social readiness from the outset. As two examples for good practice, two tools are presented that help facilitate such a process. It is planned to implement this process with the SPARTA Programs to identify possible ethical, legal and societal problems and to improve the social readiness of the solutions developed there. Finally, section 3.5 develops some initial ideas on how to structurally anchor the consideration of ethical, legal and social aspects in the future institutionalisation of cybersecurity research.

4.2 Responsible Research and Innovation

The concept of RRI has experienced a remarkably dynamic development, particularly over the course of the past decade. Starting from debates on responsible development in the area of nanotechnologies in the early 2000s, responsible (research and) innovation quickly attracted considerable attention in the academic discourse on the governance of research and innovation (Rip 2014). What is more, RRI as a concept was strongly promoted by numerous actors on the field of research and innovation policy, particularly by the European Union, culminating in the integration of RRI in Horizon 2020 as a crosscutting theme (European Commission 2014). Regardless of the different conceptualisations currently being discussed and applied, RRI in general aims to better align research and innovation with societal needs, expectations and values.

Efforts to better integrate societal and ethical aspects into research and innovation have a long-standing tradition. RRI builds on a number of these conceptual approaches, partially integrates and develops them further. Among the most influential lines of thinking, concepts and disciplinary contributions are science and technology studies (STS), technology assessment (TA) in its numerous guises, ethics of science and technology, ELSA/ELSI research, sustainable technology development, value sensitive design, responsible development, participatory and transdisciplinary research, research integrity, responsible metrics etc. (Lindner et al. 2016; Brundage and Guston 2019). In the context of EC-funded research, societal and ethical considerations were slowly integrated from the Second Framework Program FP2 (1987-1991) onwards (Rodríguez, Fisher, and Schuurbiers 2013). A key moment leading to a significant step change in actively addressing the science-society interface was the publication of EC White Paper on Governance in 2001 (European Commission 2001), arguably contributing to a "participatory turn" at least at the level of the EC's governance rhetoric (Lindner, Aichholzer, and Hennen 2016). The political background of the white paper was the increasing sense that countermeasures were needed in order to respond to the deteriorating legitimacy of the European Union and the growing distrust of citizens in the European

institutions. Science and scientific expertise were under threat as well due to a number of scandals and crises such as BSE. The solution was sought in making science socially more robust by aiming at higher levels of openness, involvement and inclusiveness. As part of this ambition, the work program "Science and Society" was established in FP6 (2002-2006), which was continued and further strengthened as "Science in Society" in FP7 (2007-2013) (de Saille 2015) and as "Science with and for Society" in Horizon 2020 (2014-2020) (Owen and Pansera 2019). Dedicated funding of projects focusing on RRI by the European Union, explicitly using the term, started in the second half of FP7 and reached a peak in the course of H2020. High-level political support of the policy concept RRI was also given by the European Council in 2014, when it officially endorsed the Rome Declaration on Responsible Research and Innovation (European Union 2014). Arguably, an important supporting factor significantly contributing to the rise of the RRI concept was a paradigm shift at the level of research and innovation policy. The Lund Declaration of 2009, which was adopted during the Swedish Presidency of the Council of the European Union and represents an important milestone in this on-going paradigm shift, called for a re-orientation of European research policy to "focus on the Grand Challenges of our time" (European Union 2009). As a consequence, policy approaches that aim to direct research and innovation towards societal needs and solutions to pressing problems, such as RRI, increasingly gained traction (Lindner and Kuhlmann 2018). This broader policy context was also conducive to the uptake of responsibility-related initiatives in a number of countries and organisations (Wittrock et al. 2021).

The probably most widely used and cited definition of RRI was presented by René von Schomberg, one of the spiritus rectors and key proponents of the concept:

Responsible Research and Innovation is a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society) (von Schomberg 2011, 9)

Partly drawing on von Schomberg's conceptual groundwork, in the context of H2020 the European Commission defines RRI as follows:

Responsible Research and Innovation (RRI) implies that societal actors (researchers, citizens, policy makers, business, third sector organisations, etc.) work together during the whole research and innovation process in order to better align both the process and its outcomes with the values, needs and expectations of society.[9]

Particularly in the early years since the official inception of RRI, the European Commission's definition of the concept was contested. A reason might be that the concept was first defined by science policy makers and agencies at the EC level, largely in a top-down manner (Zwart, Landeweerd, and van Rooij 2014), before a broader debate with the research communities could unfold. As a result, several (competing) definitions of responsible innovation were offered in the academic literature. Of these, the following received considerable attention:

Responsible innovation means taking care of the future through collective stewardship of science and innovation in the present. (Stilgoe, Owen, and Macnaghten 2013, 1570)

RRI is a higher-level responsibility or meta-responsibility that aims to shape, maintain, develop, coordinate and align existing and novel research and innovation-related processes, actors and responsibilities with a view to ensuring desirable and acceptable research outcomes (Stahl 2013, 5)

Regardless of the different perspectives and qualities of the governance of research and innovation these definitions emphasize, in can be summarised that they share the idea of the mutual interrelation of science and society with regard to social desirability, sustainability, and ethical acceptability of research and innovation. In this sense, the design of research and innovation processes should contribute to a more emphatic orientation towards social, economic and

[9] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation (accessed 12-12-2020). Between 2012 until today, the EC modified this definition repeatedly.

environmental challenges. This is to be achieved by taking better account of diverse sources of knowledge and by applying suitable procedures that promote the early and effective involvement of interest groups, users and citizens in particular. Decisions related to research and innovation should thus be made more reflexive and, overall, placed on a broader, more plural and thus more legitimate basis. Ultimately, conscious 'accountability' could re-shape the governance of research and innovation, according to which the focus is no longer on questions of technology- and innovation-induced risks and their reactive-regulatory containment, but rather on a democratically and inclusively developed understanding of what kind of futures societies are striving for by the means of innovation (Lindner et al. 2016).

In an attempt to operationalise the RRI concept, different approaches and conceptual elements have been developed. Pellé and Reber (2015) distinguish between primarily (1) process-oriented approaches that emphasize important conditions for RRI, and approaches that are based on sets of certain (2) elements or ingredients that are conducive for achieving the ambitions of RRI.

4.2.1 Process-oriented approach

Among the process-oriented approaches, which tend to be promoted by academic literature, the framework originally developed by Stilgoe, Owen, and Macnaghten (2013) has perhaps gained the most attention. In this framework, four process qualities have been defined that are broadly seen to contribute to achieving higher levels of responsibility in research and innovation practices. The process qualities or conditions anticipation, reflexivity, inclusion and responsiveness (see list below) aim to enhance actors' reflection on the way research and innovation are conducted and intend to integrate societal and future-oriented perspectives.

- **Anticipation** is about carefully examining both the intended and possible unintended consequences arising from research and innovation activities, including environmental, health-related, economic and social impacts. Anticipatory processes prompt "what if…?" questions that allow researchers and innovators to pre-pare for and respond to the various uncertainties and dilemmas built into their work.
- **Reflexivity** is about reflecting on the underlying motivations, assumptions and commitments driving research and innovation. It commits researchers and innovators to inquire and challenge the taken-for-granted assumptions structuring their work and makes them attentive to alternative ways of framing the value and societal impact of their ideas, methods and proposed solutions.
- **Inclusion** is closely related to public engagement and stakeholder involvement. It is about involving relevant societal actors in research and innovation activities from an early stage, and ensuring continuous, open dialogue about desirable and undesirable outcomes throughout the project. Inclusion serves to broaden the ideas, perspectives and world-views guiding research and innovation activities.
- **Responsiveness** is about aligning research and innovation activities with the new perspectives, insights and values emerging through anticipatory, reflexive and inclusion-based RRI processes. Responsiveness presupposes a will to learn from practical experience and a capacity to translate this learning into better, more responsible research and innovation solutions.

Source: (Nielsen et al. 2017), based on (Owen, Macnaghten, and Stilgoe 2012; Stilgoe, Owen, and Macnaghten 2013; Foley and Wiek 2017)

Numerous variations of these four process qualities or conditions have been proposed so far (for a literature overview see Burget, Bardone, and Pedaste 2017). Most notably, based on the framework, the UK Engineering and Physical Sciences Research Council (EPSRC) developed its own approach to institutionalise responsible innovation by including the so-called "AREA" framework (anticipate, reflect, engage, act)[10] in its funding guidelines.

[10] https://epsrc.ukri.org/research/framework/ (accessed Dec. 14, 2020)

4.2.2 Keys-oriented approach

Another influential operationalisation of RRI was put forward by the European Commission in 2012 (Geoghegan-Quinn 2012). The so-called key dimensions of RRI or just "the keys" appear to be more tangible than the primarily process-oriented approaches (Pellé and Reber 2015). After various modifications, the EC promoted five keys as thematic action elements in H2020[11]:

- **Public engagement** is about engaging a broad range of societal actors in the research and innovation pro-cess, including researchers, industry, policy-makers and civil society actors.
- **Open access** is about making research and innovation activities more transparent and easily accessible to the public, e.g., through open data and free access to publications.
- **Gender** is about promoting women's participation as researchers and integrating a gender dimension into research and innovation content.
- **Ethics** is about fostering research and innovation activities of high societal relevance, that comply to the highest ethical standards.
- **Science education** is about increasing society's general science literacy, e.g., by boosting children's interest in science and technology, and by equipping civil society actors with the necessary skills to more actively take part in the research and innovation process.

Source: Nielsen et al. (2017, 7)

From early on, the key dimensions were viewed critically by many observers, particularly in academia, as the package of the keys appeared to be rather disparate and arbitrary, lacking a consistent and integrative line of reasoning. Nonetheless, the keys proved to be highly performative because they seemed to be implementable, addressed well-established funding traditions and mobilised mostly independent and separate research communities. In addition, the EC put significant emphasis on the keys by integrating them in calls and urging their uptake as part of the self-evaluation requirements of participants in H2020. In this context, the MoRRI project[12] was tasked with the objective to develop a RRI monitoring and indicator system based on the RRI key dimensions (Peter et al. 2018).

Regardless of the critical debate on the different operationalisations of RRI, in practice both main approaches are being implemented in research and innovation activities since many years now, increasingly in combinations suitable for the concrete research process and context conditions at hand. Figure 8 provides an overview of the two most important operationalisations of RRI.

[11] The sixth key "governance" was dropped after the EC realised the difficulties of implementing this key. The current keys are presented at https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation (accessed Dec. 14, 2020).

[12] Monitoring the evolution and benefits of responsible research and innovation (2014-2018, contract RTD-B6-PP-00964-2013). The results are available at: https://super-morri.eu/morri-2014-2018/ (accessed Dec. 14, 2020).

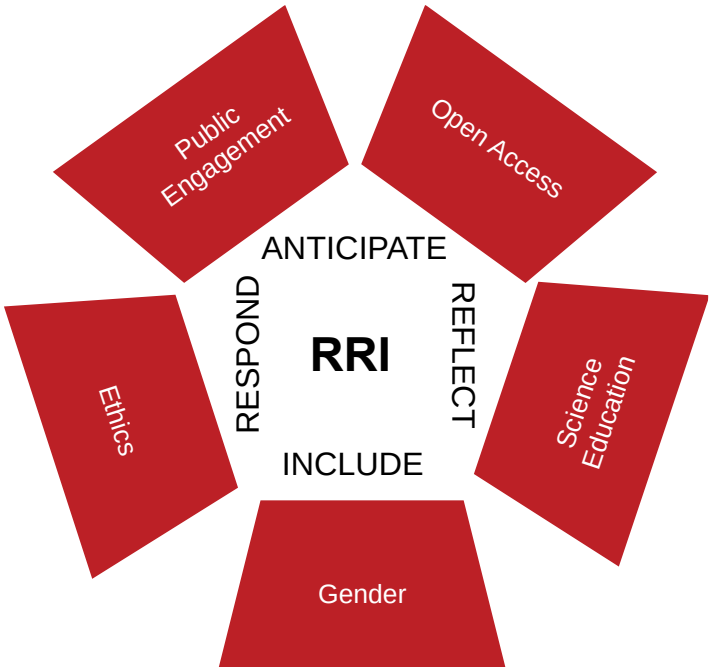


Figure 9: Conditions and key dimensions of RRI

4.3 From technology readiness to societal readiness of emerging technologies

In contrast to other approaches RRI seeks to move the mere assessment and reflection towards active support of the societal uptake of beneficial innovations. Rather than just protecting society from undesirable consequences, RRI aims to address societal challenges through the use of technology, i.e., the goal is to produce socially desirable innovations that address specific public needs (von Schomberg 2011). But how can these effects of technological development on society be measured, how can it be decided whether a technology is compatible with the needs and interests of citizens?

Concepts have been developed for the management of technology development to determine its usability and market readiness. Of these, the concept of Technology Readiness Levels (TRL), developed by NASA in the late 1970s, is certainly particularly influential because it allows to measure to what extent technology is mature enough for the intended application. The scale is arranged in 9 evolutionary (linear) stages, showing how far a technology is from being ready for use in its intended operational environment. Following the recommendation of High-Level Expert Group on Key Enabling Technologies (2011) the European Commission decided to adopt TRL as a tool for organizing innovation policy and funding and consequently applied this instrument to measure and govern the contribution of innovation in the EU Horizon 2020 program (European Commission 2012). There was, however, extensive criticism of the adoption of TRL by the European Union because even inside the technological field "concreteness and sophistication of the TRL scale gradually diminished as its usage spread outside its original context" (Héder 2017, 18).

Another criticism that is especially relevant here is the fact that TRL only measures technical performance and does not consider the contribution of a technology to solving societal issues or their societal fit. To address this imbalance, it was suggested to include societal aspects in technology modelling and testing, with a view to readiness to adopt the resulting innovation. With this in mind, Innovation Fund Denmark (n.d.) proposed measuring the „Societal Readiness Level“ (SRL) of a certain technology, product, process, or intervention. The underlying premise is that every innovation - be it technical or social - requires integration into the social environment to be successful. The scale for SRL is structured in the same way as the scale for TRL, with 9 stages ranging from concept to full integration into society systems (Table 1).

Maturity	Description
SRL 1	Identification of the generic societal need and associated readiness aspects
SRL 2	Formulation of proposed solution concept and potential impacts; appraisal of societal readiness issues; identification of relevant stakeholders for the development of the solution
SRL 3	Initial sharing of the proposed solution with relevant stakeholders (e.g. through visual mock-ups): a limited group of the society knows the solution or similar initiatives
SRL 4	Solution validated through pilot testing in controlled environments to substantiate proposed impacts and societal readiness: a limited group of the society tests the solution or similar initiatives
SRL 5	Solution validated through pilot testing in real or realistic environments and by relevant stakeholders: the society knows the solution or similar initiatives but is not aware of their benefits
SRL 6	Solution demonstrated in real world environments and in co-operation with relevant stakeholders to gain feedback on potential impacts: the society knows the solution or similar initiatives and awareness of their benefits increases
SRL 7	Refinement of the solution and, if needed, retesting in real world environments with relevant stakeholders: the society is completely aware of the solution's benefits, a part of the society starts to adopt similar solutions
SRL 8	Targeted solution, as well as a plan for societal adaptation, complete and qualified; society is ready to adopt the solution and have used similar solutions on the market
SRL 9	Actual solution proven in relevant societal environments after launch on the market; the society is using the solution available on the market

Table 1: Socio-technical definition of Societal Readiness Levels, adapted from Innovation Fund Denmark (Source: Bruno 2020)

It is currently an open question whether quantifying SRL is really useful. However, a (qualitative) discussion of elements of societal readiness that is oriented towards the criteria of RRI can at least allow for a rough assessment. Taken together, the two Readiness Level scales can form a building block of a unifying framework that can be used to assess and compare the potential of new (and existing) digital technologies to promote innovation in a sustainable fashion. The mapping shown in Figure 9 can give a good impression of the goodness of alternative solutions, although it can be argued that the two dimensions (TRL/SRL) are not completely independent of each other. Bruno (2020) has even suggested adding more "readiness" dimensions (organisation readiness, legal readiness) to the mapping to improve the quality of the assessment and to facilitate the decision between alternatives.

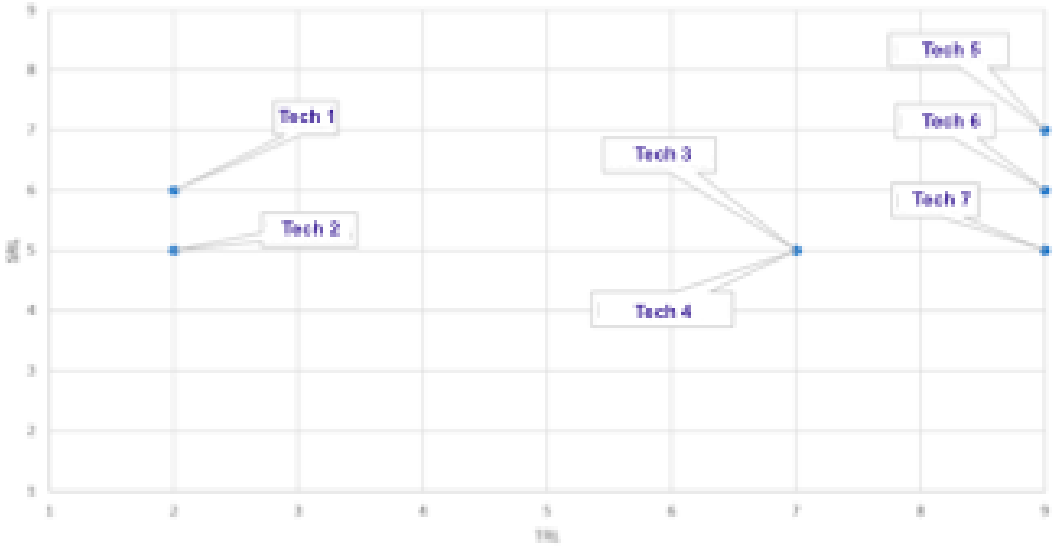


Figure 10: Two-dimensional mapping of technologies on the SRL and TRL scales

From the context of RRI research, there is now a whole range of methods and instruments for assessing social readiness – even if the term is rarely used. These range from simple questionnaires to sophisticated workshop concepts and computer-based processes, following different approaches to conceptualise measure societal impacts and with different target groups.[13]

Either way, an effective tool requires a flexible design that recognises the multifaceted and pluralistic nature of project-based research that we also see in cybersecurity:

- It needs to be detailed enough to stimulate appropriate reflection and action;
- it must be general enough to be applicable in different application contexts;
- it must effectively enable participants in research projects to reflect on the social appropriateness of their work at critical stages of the project life cycle.

4.4 A methodology for systematically increasing societal readiness of emerging technologies

In this section we are presenting a process (see Figure 11), developed in the H2020 funded NewHoRRIzon project, that is intended as an instrument to guide researchers and decision makers through the examination of RRI-related dimension.

[13] The probably most complete overview of these tools is given on the repository developed by the RRI tools project: https://rri-tools.eu/. A very user-friendly selection of tools is provided by the "RRI Cook Book" (FoTRRIS Project 2018).

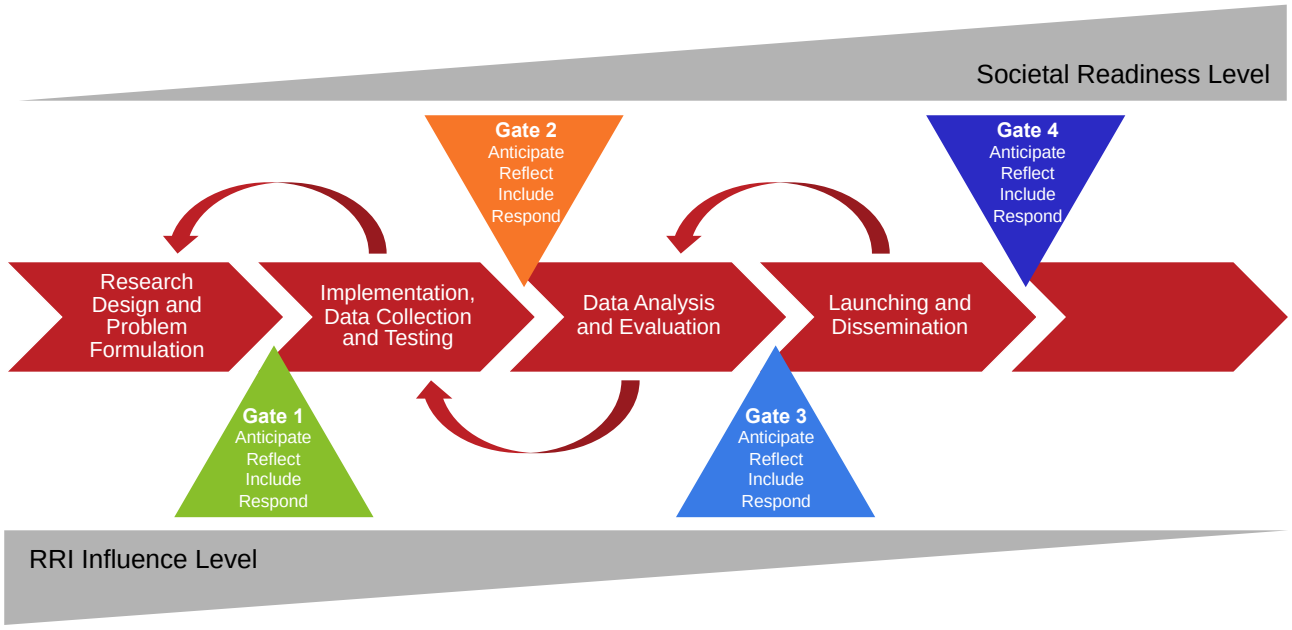


Figure 11: Elements of a RRI based reflection process (Nielsen et al. 2017)

The first important question is *when* an assessment of the societal readiness should be made. To make sure that the assessment can unfold its full potential is must be ensured that it is not understood as a one-off action but as a continuous process that should be carried out several times in whole or in part during the product life cycle or the implementation of the concrete technical system.

The greatest opportunities for making a technical system socially acceptable typically arise in the earliest development phase, when the research question to be addressed and the problem to be solved are defined. During this phase, however, concrete impacts of the application are often difficult or impossible to foresee. This is easier in later development phases, however, when fundamental design decisions have long been made and can no longer be changed easily and only with great effort and expense. This means that researchers and innovators need to invest considerable effort in RRI early in the project life cycle in order to achieve a high level of societal readiness at the end of the project (Genus and Stirling 2018). Solving this dilemma requires a well-developed "sociological imagination" (Mills 2000), requiring critical and sometimes abstract thinking about the complex ways in which the proposed project may influence (and be influenced by) wider society. In the field of technology assessment, this is referred to as the "Collingridge dilemma": “When change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult, and time-consuming“ (Collingridge 1980, p. 11).

A second important question concerns the *process design* and its *embedding in the organisation*. In order to align the reflection process with traditional concepts of R&D management, a stage-gating-inspired approach is proposed, where a project is divided into different stages or phases separated by decision points called gates (Cooper 2001). At each gate, a decision is made on the continuation of the project using previously defined criteria. Typically, this decision is taken on the basis of forecasts and available data on expected business development, the resources needed for further development and the costs incurred. It usually aims to increase the efficiency of development and optimise market opportunities. Stilgoe, Owen, and Macnaghten (2013) have suggested that such a stage-gating approach can also be used to reduce legal, ethical and societal risks and to improve the societal readiness of research and innovation activities by adding additional RRI-related criteria.

Although the process for reflection can also be used by the individual researcher, it should be integrated into the regular processes of a research and development unit and have strong commitment and support from the management of the organisation. When carrying out the process,

not only the core development team should be involved, but also the competent management, other relevant organisational units, but in particular representatives of the affected citizens.

For issues of "societal readiness", the definition of the development phases and the gates does not necessarily have to correspond to the definition used for typical project management tasks. However, following established structures makes it easier to integrate new elements into existing processes. This helps to improve acceptance both among management, which has to approve the necessary adjustments, and among developers, who have to take on additional tasks besides their actual core activities.

For the sake of illustration, we are distinguishing four separate phases that are common to most research-driven projects:

- **Phase 1** includes the identification and description of the problem to be solved, the ideation process in which different approaches to solving the problem are developed and the translation of these ideas into a research and development concept, as well as the determination of the appropriate procedures and data for this.
- **Phase 2** includes all activities related to implementation, data collection and experimental testing.
- **Phase 3** covers data analysis, evaluation and interpretation of the empirical results.
- **Phase 4** involves the market introduction and the dissemination of results to relevant stakeholders, researchers and the public.

This is not necessarily a linear process, because in reality these phases are not always sequential. Sometimes action precedes a precise theoretical understanding. Sometimes action triggers the development of new ideas. Finally, there will be feedback loops between the phases. All this has to be taken into account; after all, we are dealing with an iterative process in which the "gates" play an important role as control and decision points.

After what was said before about the control dilemma, it is clear that the first gate is particularly important. At this point in time, before the first line of code is written, a particularly careful and comprehensive evaluation must take place, as this influences the overall direction of development.

How is this process implemented in practice? For the assessment of societal readiness, the RRI-relevant dimensions need to be reflected in a systematic way. To this end, the project has identified and systematised questions from the existing literature (Nielsen et al. 2017). A separate questionnaire is created for each of the gates. In each questionnaire, (generic) questions were identified for the five RRI key elements addressing the four RRI conditions (Table 2).

Gate #	Anticipate	Reflect	Include	Respond
Public Engagement	Questions	…	…	Questions
Open Access	…	…	…	…
Science Education	…	…	…	…
Gender	…	…	…	…
Ethics	Questions	…	…	Questions

Table 2: Structure of a questionnaire for each gate

In order to pass the gate and to move from one phase to the next, researchers and stakeholders should thoroughly consider the issues and make a careful assessment. They should adapt the questions for the specific context and ideally come up with additional questions that are of particular relevance to their own project. Sometimes it is also important to argue why a certain aspect is not as relevant as another in a given situation. For use in the cybersecurity context, the questionnaires

presented in the appendix would have to be adapted and supplemented in cooperation with experts from the field.

It is, however, one thing to think theoretically about the level of social readiness of research and innovation, it is quite another to transfer the results of these considerations for one's own research and development work. It has already been pointed out that each researcher could make the assessment for himself, but it makes much more sense to do it in a participatory way.

In recent years quite a number of tools have been developed that support the reflection process. Though these tools cannot automatically assess societal readiness on the basis of standardised data, they can help guiding participants and stakeholders through the process, presenting the relevant questions and linking them to existing additional resources and tools. The latter is important because one does not have to reinvent assessment techniques for each aspect, but can use the wealth of research results.

4.5 The way forwards – preliminary reflections on mainstreaming RRI in Cybersecurity

In their "Joint declaration on mainstreaming RRI across Horizon Europe" (Gerber et al. 2020) leading European researchers have made clear that RRI is an „on-going process of aligning research and innovation to societal values, needs and expectations" have argued in favour of a stronger institutionalization of RRI making use of the conceptual and practical work that has been achieved since the political adoption of RRI in the early 2010s. Such an institutionalization seems necessary on different levels.

First and foremost, with regard to the soon to be established structures of European cybersecurity research, i.e., the European Cybersecurity Competence Network, the European Cybersecurity Centre, and the National Coordination Centres. These bodies, which are instrumental in determining the direction and character of future research, should establish structures and mechanisms from the outset that ensure early, comprehensive and honest consideration of legal, ethical and societal issues.

The institutionalisation of RRI at European program level is a necessary but not necessarily sufficient step. All players in the cybersecurity ecosystem must also adapt to the requirements of RRI. While this adaptation can take place in response to externally formulated requirements (i.e., those made in the EU funding conditions) it should be a medium to long-term goal that RRI thinking and practices become part of institutional DNA.

In the following section, we outline some preliminary ideas for mainstreaming RRI in cybersecurity research. They are based on considerations from other contexts but can be the starting point for a debate for the cybersecurity ecosystem as well.

In the above mentioned „Joint declaration" the authors see a risk, that in "Horizon Europe" the RRI agenda might be diluted with the end of the "Science with and for Society" program and that the results of the program are endangered, all at a critical time when institutional change actions are starting to gain momentum. From the advice that the expert group is giving, the following is also relevant for RRI/ELSA in future cybersecurity research (Gerber et al. 2020):

- **EU Program Level**
  - Since ethical, legal and societal issues are generally relevant in cybersecurity research and innovation the future Horizon Europe calls should explicitly ask to outline how projects relate to RRI, based on guidelines for how to embed RRI effectively and how to measure societal impact. The proper inclusion of RRI actions must involve specified tasks, deliverables, milestones and budgets in order to be convincing.
  - Cybersecurity research should therefore include interdisciplinary collaboration between the technical sciences, law and social sciences and humanities. The structure chosen in SPARTA with a dedicated RRI/ELSA work package on the one

hand and "embedded" social scientists and lawyers in the technical work packages on the other hand can serve as a model.
    - It should be foreseen that deliberative and participatory methods (e.g., focus groups with stakeholders, co-creation workshops etc.) are integrated in the technical development work. Mutual learning of researchers from both, the technical as well as the social and legal disciplines, can improve the overall effectiveness of this approach and the quality of the results.
- **EU Institutions Level**
    - The emerging European institutions or agencies, the European Cybersecurity Competence Centre (ECCC) and the National Coordination Centres (NCC) should have a mandate to build and maintain ELSA elements, procedures and methods in cybersecurity research. They should in particular be able to advise, train, consult, assess and provide quality control and be a resource for those who include RRI-related activities in their activities. In that capacity the emerging institutions should provide expertise for the assessment of these aspects of proposals and project activities, and for relevant committees and boards. (Gerber et al. 2020)
- **Other Institutions Level**
    - The most difficult question in the context of mainstreaming ELSA/RRI aspects in cybersecurity research is certainly how to engage the multitude of academic, but especially industrial, actors in the spirit of RRI. A fundamental cultural change, or “deep institutionalisation“ (Randles 2017) is necessary for these actors, which is the opposite of today's widespread practice of e.g., ad hoc implementation of individual governance instruments or devices. Such a superficial institutionalisation is not able to transform organisations towards more “responsible” normative goals.

Implementing such deep institutionalisation, however, is not an easy task. Studies (e.g., Bamberger and Mulligan 2015) have shown that there is a strong interaction between management practices and different kinds of (hard and soft) regulation. There is some evidence that even in hierarchical organisations, it is not possible to establish RRI-compatible processes and behaviours. Rather, external measures are needed to enforce a certain organisational behaviour (e.g., mandatory procurement rules) as well as internal measures (e.g., adapted structures, staff trainings, RRI related KPIs and explicit incentives) (Steen and Nauta 2020).

In the remaining time of the SPARTA project, measures at the different levels should be selected or developed and - if possible - tested. In particular, the process of improving societal readiness can be experimented with in cooperation with the SPARTA programs, with the aim of further refining the procedures as well as the questionnaires.

Bibliography

Andersen, Henrik. 2017. "Conceptions of Responsible Research and Innovation in Funding Processes: A case study of Convergence Environments at the University of Oslo Life Science." Master thesis, TIK Centre for Technology, Innovation and Culture, University of Oslo. https://www.duo.uio.no/bitstream/handle/10852/59569/1/Master_thesis_Andersen.pdf.

Bamberger, Kenneth A., and Deirdre K. Mulligan. 2015. *Privacy on the ground: Driving corporate behavior in the United States and Europe*. Cambridge, Mass.; London: The MIT Press.

Bendiek, Annegret, Raphael Bossong, and Matthias Schulze. November 2017. *The EU's revised cybersecurity strategy: halfhearted progress on far-reaching challenges.* Stiftung Wissenschaft und Politik (Berlin). https://nbn-resolving.org/urn:nbn:de:0168-ssoar-55103-4.

Brundage, Miles, and David H. Guston. 2019. "Understanding the movement(s) for responsible innovation." In *International Handbook on Responsible Innovation: A Global Resource*, edited by René von Schomberg and Jonathan Hankins, 102-121. Cheltenham: Edward Elgar.

Bruno, Ilenia, Georges Lobo, Beatrice Valente Covino, Alessandro Donarelli, Valeria Marchetti, Anna Schiavone Panni, and Francesco Molinari. 2020. "Technology readiness revisited: a proposal for extending the scope of impact assessment of European public services." ICEGOV 2020:

Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance, Athens, Greece.

Burgess, J. Peter, Genserik Reniers, Koen Ponnet, Wim Hardyns, and Wim Smit, eds. 2018. *Socially Responsible Innovation in Security: Critical Reflections*. London and New York: Routledge.

Burget, Mirjam, Emanuele Bardone, and Margus Pedaste. 2017. "Definitions and Conceptual Dimensions of Responsible Research and Innovation: A Literature Review." *Science and engineering ethics* 23 (1): 1–19. https://doi.org/10.1007/s11948-016-9782-1.

Callon, Michel, Pierre Lascoumes, and Yannick Barthe. 2011. *Acting in an uncertain world: An essay on technological democracy*. Cambridge, Mass. and London: MIT Press.

CEN. 2017. *Ethics assessment for research and innovation – Part 2: Ethical impact assessment framework.* European Committee for Standardization (Brussels). ftp://ftp.cencenelec.eu/EN/ResearchInnovation/CWA/CWA17214502.pdf.

Collingridge, David. 1980. *The social control of technology*. London: Pinter.

Cooper, Robert G. 2001. *Winning at new products: Accelerating the process from idea to launch*. Cambridge, Mass: Perseus.

de Saille, S. 2015. "Innovating innovation policy: the emergence of 'Responsible Research and Innovation'." *Journal of Responsible Innovation* 2 (2): 152-168. https://doi.org/10.1080/23299460.2015.1045280.

European Commission. 25 July 2001. *European Governance: A White Paper.* (Brussels). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF.

---. 26 June 2012. *A European strategy for Key Enabling Technologies – A bridge to growth and jobs, COM(2012) 341 final.* (Brussels). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0341:FIN:EN:PDF.

---. 2014. *Horizon 2020 Work Programme 2014-2015: Science with and for Society. (European Commission Decision C (2014)4995 of 22 July 2014).* (Brussels). https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-swfs_en.pdf.

European Union. July 2009. *The Lund Declaration: Europe must focus on the Grand Challenges of Our Time.* Swedish Presidency of the Council of the European Union (Brussels). https://www.vr.se/download/18.6969eb1a16a5bec8b59338/1556886570218/Lund%20Declaration%202009.pdf.

---. 21 November 2014. *Rome Declaration on Responsible Research and Innovation in Europe.* Italian Presidency of the Council of the European Union (Brussels). https://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf.

Foley, Rider, and Arnim Wiek. 2017. "Bridgework ahead! Innovation ecosystems vis-à-vis responsible innovation." *Journal of Nanoparticle Research* 19 (2): 1-16. https://doi.org/10.1007/s11051-017-3770-5.

FoTRRIS Project. March 2018. *How to Co-Create RRI Projects.* http://fotrris-h2020.eu/wp-content/uploads/2018/08/FOTRRIS-Cookbook-RRI.pdf.

Genus, Audley, and Andrew Stirling. 2018. "Collingridge and the dilemma of control: Towards responsible and accountable innovation." *Research Policy* 47 (1): 61-69. https://doi.org/10.1016/j.respol.2017.09.012.

Geoghegan-Quinn, Mairé. 26 April 2012. *Commissioner Geoghegan-Quinn Keynote speech at the "Science in Dialogue" Conference Odense.* http://ec.europa.eu/archives/commission_2010-2014/geoghegan-quinn/headlines/speeches/2012/documents/20120423-dialogue-conference-speech_en.pdf.

Gerber, Alexander, Ellen-Marie Forsberg, Clare Shelley-Egan, Rosa Arias, Stephanie Daimer, Gordon Dalton, Ana Belén Cristóbal, Marion Dreyer, Erich Griessler, Ralf Lindner, Gema Revuelta,

Andrea Riccio, and Norbert Steinhaus. 2020. "Joint declaration on mainstreaming RRI across Horizon Europe." *Journal of Responsible Innovation* 7 (3): 708-711. https://doi.org/10.1080/23299460.2020.1764837.

Héder, Mihály. 2017. "From NASA to EU: the evolution of the TRL scale in Public Sector Innovation." *The Innovation Journal: The Public Sector Innovation Journal* 22 (2): article 3. https://www.innovation.cc/discussion-papers/2017_22_2_3_heder_nasa-to-eu-trl-scale.pdf.

High-Level Expert Group on Key Enabling Technologies. June 2011. *Final Report.* European Commission (Brussels). https://www.kowi.de/en/Portaldata/2/Resources/fp7/hlg_kets_final_report_en.pdf.

Innovation Fund Denmark. n.d. *Societal Readiness Levels (SRL) defined according to Innovation Fund Denmark.* (Aarhus). https://innovationsfonden.dk/sites/default/files/2019-03/societal_readiness_levels_-_srl.pdf.

Jirotka, Marina, Barbara Grimpe, Bernd Stahl, Grace Eden, and Mark Hartswood. 2017. "Responsible research and innovation in the digital age." *Communications of the ACM* 60 (5): 62-68. https://doi.org/10.1145/3064940.

Knockaert, Manon, Jean-Marc Van Gyseghem, Michael Friedewald, and Ralf Lindner. 31 January 2020. *Ethical, Legal and Societal Aspects.* SPARTA Project (EU H2020, GA 830892).

Kupper, Frank, Pim Klaassen, Michelle Rijnen, Sara Vermeulen, and Jacqueline Broerse. 30-03-2015 2015. *Report on the quality criteria of Good Practice Standards in RRI.* RRI Tools Project (EU FP7, GA 612393). https://www.fosteropenscience.eu/sites/default/files/original/4277.pdf.

Kupper, Frank, Pim Klaassen, Michelle Rijnen, Sara Vermeulen, Remco Woertman, and Jacqueline Broerse. 29-06-2015 2015. *A catalogue of good RRI practices.* RRI Tools Project (EU FP7, GA 612393). https://www.mistraurbanfutures.org/sites/mistraurbanfutures.org/files/catalogue-of-good-rri-practices.pdf.

Lindner, Ralf, Georg Aichholzer, and Leonhard Hennen. 2016. "Electronic Democracy in Europe: An Introduction." In *Electronic Democracy in Europe: Prospects and Challenges of E-Publics, E-Participation and E-Voting*, edited by Ralf Lindner, Georg Aichholzer and Leonhard Hennen, 1-17. Cham: Springer.

Lindner, Ralf, Kerstin Goos, Sandra Güth, Oliver Som, and Thomas Schröder. 2016. *„Responsible Research and Innovation“ als Ansatz für Forschungs-, Technologie- und Innovationspolitik – Hintergründe und Entwicklungen: TA-Vorstudie.* Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (Berlin). http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Hintergrundpapier-hp022.pdf.

Lindner, Ralf, and Stefan Kuhlmann. 2018. "Navigieren in Richtung Responsible Research and Innovation: Governanceprinzipien zur strategischen Reflexion." In *"Grand Challenges" meistern. Der Beitrag der Technikfolgenabschätzung*, edited by Michael Decker, Ralf Lindner, Stephan Lingner, Constanze Scherz and Mahshid Sotoudeh, In Gesellschaft – Technik – Umwelt, 97-108. Baden-Baden: Edition Sigma.

Mills, C. Wright. 2000. *The sociological imagination*. Oxford and London: Oxford University Press.

Nielsen, Mathias Wullum, Niels Mejlgaard, Emil Alnor, Eric Griessler, and Ingeborg Meijer. 30 April 2017. *Ensuring Societal Readiness. A Thinking Tool.* NewHoRRIzon Project (EU H2020, GA 741402). https://www.thinkingtool.eu/Deliverable_6.1_Final_April%2030_THINKING_TOOL.pdf

Owen, Richard, Phil Macnaghten, and Jack Stilgoe. 2012. "Responsible research and innovation: From science in society to science for society, with society." *Science and Public Policy* 39 (6): 751-760. https://doi.org/10.1093/scipol/scs093.

Owen, Richard, and Mario Pansera. 2019. "Responsible innovation: process and politics." In *International Handbook on Responsible Innovation: A Global Resource*, edited by René von Schomberg and Jonathan Hankins, 35-48. Cheltenham: Edward Elgar.

Pellé, Sophie, and Bernard Reber. 2015. "Responsible innovation in the light of moral responsibility." *Journal on Chain and Network Science* 15 (2): 107-117. https://doi.org/10.3920/JCNS2014.x017.

Peter, Viola, Frederic Maier, Niels Mejlgaard, Carter Bloch, Emil B. Madsen, Erich Griessler, Milena Wuketich, Ingeborg Meijer, Richard Woolley, Ralf Lindner, Susanne Bührer, Angela Jäger, Lena Tsipouri, and Jack Stilgoe. 2018. *Monitoring the evolution and benefits of responsible Research and Innovation. Summarising insights from the MoRRI project*. Luxembourg: Publications Office of the European Union.

Petratos, Pythagoras. 2014. "Cybersecurity in Europe: Cooperation and Investment." In *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*, edited by Elias G. Carayannis, David F.J. Campbell and Marios Panagiotis Efthymiopoulos, 279-301. New York, Heidelberg: Springer.

Randles, Sally. 12 January 2017. *Deepening 'Deep Institutionalisation'.* JERRI Project (EU H2020, GA 709747). https://www.jerri-project.eu/jerri-wAssets/docs/deliverables/wp-1/JERRI_Deliverable_D1_2_Deepening-Deep-Institutionalisation.pdf.

Rip, Arie. 2014. "The Past and Future of RRI." *Life Sciences, Society and Policy* 10: 17. https://doi.org/10.1186/s40504-014-0017-4.

Rodríguez, Hannot, Erik Fisher, and Daan Schuurbiers. 2013. "Integrating science and society in European Framework Programmes: Trends in project-level solicitations." *Research Policy* 42 (5): 1126-1137. https://doi.org/10.1016/j.respol.2013.02.006.

von Schomberg, René, ed. 2011. *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*. Luxembourg: Publications Office of the European Union.

Spiekermann, Sarah, Jana Korunovska, and Marc Langheinrich. 2019. "Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers." *Proceedings of the IEEE* 107 (3): 600 - 615. https://doi.org/10.1109/JPROC.2018.2866769.

Stahl, Bernd Carsten. 2013. "Responsible Research and Innovation: The Role of Privacy in an Emerging Framework." *Science and Public Policy* 40 (6): 708-716. https://doi.org/10.1093/scipol/sct067.

Stahl, Bernd Carsten, Grace Eden, Catherine Flick, Marina Jirotka, Quang A. Nguyen, and Job Timmermans. 2015. "The Observatory for Responsible Research and Innovation in ICT: Identifying Problems and Sharing Good Practice." In *Responsible Innovation 2*, edited by Bert-Jaap Koops, Ilse Oosterlaken, Henny Romijn, Tsjalling Swierstra and Jeroen van den Hoven, 105-120. Cham: Springer.

Steen, Marc, and Joram Nauta. 2020. "Advantages and disadvantages of societal engagement: a case study in a research and technology organization." *Journal of Responsible Innovation* 7 (3): 598-619. https://doi.org/10.1080/23299460.2020.1813864.

Stilgoe, Jack, Richard Owen, and Phil Macnaghten. 2013. "Developing a framework for responsible innovation." *Research Policy* 42 (9): 1568-1580. https://doi.org/10.1016/j.respol.2013.05.008.

Wittrock, Christian, Ellen-Marie Forsberg, Auke Pols, Philip Macnaghten, and David Ludwig. 2021. *Implementing Responsible Research and Innovation: Organisational and National Conditions*.*SpringerBriefs in Ethics*. Cham: Springer International.

Zwart, Hub, Laurens Landeweerd, and Arjan van Rooij. 2014. "Adapt or perish? Assessing the recent shift in the European research funding arena from 'ELSA' to 'RRI'." *Life sciences, society and policy* 10 (11). https://doi.org/10.1186/s40504-014-0011-x.

Chapter 5 Security and Public Order criteria under EU Investment Framework Regulation

5.1 Introduction

The way to affect the integrity of such systems or networks is by gaining access to the underlying infrastructure, such as internet cables, telephone wires or towers, signal retransmission stations etc. A physical access to infrastructure and installation of additional devices or equipment capturing or copying data is a part of spy-craft and unauthorised access to such infrastructure usually leads to actions of criminal justice. However, the ownership of such infrastructure, be it an ownership of a telecommunications firm or a TV station, creates a different cybersecurity threat – threat of gaining unlimited access to data that goes through such infrastructure or power to affect the contents of such information through management (e.g., disinformation through TV/radio station or newspaper). It is relatively easy to assess and evaluate the legality and impact of physical access to infrastructure. Whereas issues related to ownership of infrastructure or assets that might cause potential cybersecurity or disinformation concerns are complex and nuanced, because they have to be addressed before such transaction is completed and long before any damage (if any) has manifested itself. Moreover, when a new owner is from another country, he usually also enjoys the protection given to foreign investor, which requires balancing between liberal ideas and movement of capital on the one hand and due security and public order concerns on the other.

The EU is built on idea of liberalism. For a long time, the EU was the bulwark behind open and most liberal trade and investment regime of the world. According to OECD FDI Regulatory Restrictiveness Index (OECD, 2020) the EU member states are among the countries with the world's most open investment regimes for foreign investment (from 0.004 in Luxemburg to 0.106 in Austria, where 0 is he least restrictive and 1 – the absolutely restrictive). The importance of open investment regime is enshrined as one of the fundamental rights of the EU – free movement of capital. Article 63 of the TFEU prohibits all restrictions on the movement of capital between Member States. It also prohibits restrictions on the movement of capital between Member States and third countries.

However, in 2017 the European Commission in its *Reflection Paper on Harnessing Globalisation* indicated that "concerns have recently been voiced about foreign investors, notably state-owned enterprises, taking over European companies with key technologies for strategic reasons" and that such "concerns need careful analysis and appropriate action" ((European Commission, 2017, p. 17).

Although the Reflection Paper did not mention Peoples' Republic of China by name, it was the investments of Chinese state-owned enterprises that caused such concerns by the EU. According to the data from Rhodium Group, during the period before drafting of the Reflection Paper, Chinese state-owned investors accounted to more than 70 percent of total investment in 2010-2015, with the level dropping to 36% in 2016 (Rhodium Group, the Mercator Institute for China Studies, p. 12). In September 2017 the European Commission announced the *Proposal for a Regulation of the Regulation of the European Parliament and of the Council establishing a framework for screening of foreign direct investments into the European Union* (2017) and corresponding *Communication Welcoming Foreign Direct Investment while Protecting Essential Interests* (European Commission, 2017). The Regulation was passed relatively fast and on 19 March 2019 the Regulation establishing a framework for the screening of foreign direct investments into the Union (hereinafter - Framework Regulation) was adopted (Regulation (EU) 2019/452, 2019).

The Regulation established a framework for the screening by Member States of foreign direct investments into the Union on the grounds of security or public order and for a mechanism for cooperation between Member States, and between Member States and the Commission, with regard to foreign direct investments likely to affect security or public order (Article 1 of the Framework Regulation). It became applicable from 11 October 2020 (Article 17 of the Framework Regulation).

The Framework Regulation is clear that the decision on the screening of foreign direct investment on the basis of national security or essential security interests as well as responsibility lies within individual Member States (Recitals 7 and 8, Article 1(2) of the Framework Regulation). That includes determination for the Member States on what exactly constitutes security and public order for each individual member state. Although the Framework Regulation does not provide the list of what constitutes security or public policy, nor it intends to do so, Article 4 of the Framework Regulation provides a non-exhaustive list of the factors that might be relevant in considerations done by Member States.

Overall, the Framework Regulation reflects the EU wide legislative solution to the legal challenge of foreign investment, which might be potentially harmful to security or public interests of Member States. It illuminates which sectors and assets should or can raise security and public order concerns. Moreover, it serves as a template or at the very least EU level legal instrument for the bulk of the EU Member States which do not have any legal instruments to deal with potentially harmful foreign investment under their national legislation.

At the time of this research there was no public information on implementation of the Framework Regulation, neither on what foreign direct investments were considered to be a security or public order risks while applying this Regulation. Recital 32 and Article 5(3) of the Framework Regulation indicate that Commission shall make public annual reports concerning implementation of the Framework Regulation. Until the first report of implementation of the Framework Regulation (which will not be done before April of 2021), the contents of security and public order criteria can be inferred from 2 sources: texts of official documents and positions of the EU institutions and practice of the CJEU in cases dealing with limitation of free movement of capital (Article 65 of the TFEU).

5.2 Textual analysis of security and public policy criteria under EU law

The overall idea of the European Union is to contribute to progress of global liberalisation and in particular to the progressive abolition of restrictions on international trade and on foreign direct investment (Article 206 of the TFEU). As EU wanted to maintain open investment environment on the one hand, but also recognised the need to address concerns of security and public policy related to acquisitions of key technologies, infrastructure or assets by state-owned investors, the Framework Regulation indicates assets and sectors which are considered significant for security and public policy reasons for member states, as well as the EU as a whole.

The Framework Regulation emphasises on several occasions, that it is the sole responsibility of a member states to safeguard its security and public order (Recitals 7, 8, 17, 19 and Article 1(2) of the Framework Regulation) thus indicating that it will be a member state that will have to defend its decision on measures adopted during or after the screening of foreign direct investment from the challenges. However, as only 15 out of 27[14] EU Member States have notified the Commission about the existence of screening mechanisms in November of 2020[15], the Framework Regulation also serves as a guide for Member States that do not have such screening regulations in assessing possible risks of foreign direct investments to their national and public order concerns (Recital 12 of the Framework Regulation).

Article 4(1) of the Framework Regulation provides the exemplary list of assets and sectors prone to security and public order consideration of Member States, whereas Article 8 – indicates programmes, projects and sectors which are prone to security and public order consideration of the EU as a whole.

[14] Excluding United Kingdom, which altough have screening mechanism is not a member of the European Union anymore.

[15] List of screening mechanisms notified by Member States under Framework Regulation, [https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157946.pdf

5.2.1 Sectors or assets that might cause security or public order concerns

Article 4(1) of the Framework Regulation indicates 5 sets of sectors or assets, which might raise security and public order concerns for the Member States. First of all, Article 4(1) of the Framework Regulation indicates critical infrastructure as a sector, where foreign direct investment might affect national and or public order of member states. The Framework Regulation describes critical infrastructure broadly:

> *"physical or virtual, including energy, transport, water, health, communications, media, data processing or storage, aerospace, defence, electoral or financial infrastructure, and sensitive facilities, as well as land and real estate crucial for the use of such infrastructure".*

The term 'critical infrastructure' is a term prescribed in Article 2 of the Directive 2008/114/EC (2008) and means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. Although Directive 2008/114/EC (2008) concentrates on the energy and transport sectors (Recital 5 and Article 3(3) of the Council Directive 2008/114/EC), the Framework Regulation indicates that such critical infrastructure goes beyond energy and transportation and includes health, communications, media, data processing or storage, aerospace, defence, electoral or financial infrastructure, and sensitive facilities. Such expansive notion of 'critical infrastructure' under the Framework Regulation, especially including communications, data processing or storage, enables Member States to deal with potential cybersecurity threats, whereas inclusion of media and electoral infrastructure – to address potential disinformation threats even before they have manifested themselves, i.e. in the outset of investment activities in such critical infrastructure.In March of 2020 the Commission issued Guidance (European Commission, 2020), whereas it stressed out the importance of health sector, noting that in the context of Covid-19 emergency, there might be risk of attempts to acquire the healthcare capabilities or related industries such as research establishments via foreign direct investment. The Commission provided guidance to member states, indicating that Member States might consider using screening mechanism or introduce restrictions on acquisition of companies whose shares are traded on capital markets, if their valuation is below their true or intrinsic value. The Commission in particular urged Member States to be vigilant in avoiding sell-off of Europe's business and industrial actors, including SME during Covid-19 crisis. Although there is no public information on whether any EU member state applied any restrictions on foreign direct investments in health sector, but the fact of issuance of such guidance indicates that the Commission will use the Framework Regulation as a basis for guiding the member states on possible or permissible actions in limiting foreign direct investment that might affect security or public order interests.

Finally, insofar as critical infrastructure is concerned, it should be also noted that the EU is planning to adopt a legislative proposal for additional measures on Critical Infrastructure Protection (Commission Work Programme, 2020), which might include a renewed and more detailed list on what is considered as critical infrastructure from the point of view of the EU.

Secondly, Article 4(1) of the Framework Regulation indicates that critical technologies and dual use items might affect security or public order concerns of member states. According to Council Regulation (EC) No 428/2009 (2009), dual use items means:

> *"items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices"* (Article 2(1)).

Article 4(1) of the Framework Regulation narrows down the industries and fields, where technology is deemed to be of importance to security and public order considerations. It includes artificial intelligence, robotics, semiconductors, cybersecurity, aerospace, defence, energy storage, quantum and nuclear technologies as well as nanotechnologies and biotechnologies.

Thirdly, Article 4(1) of the Framework Regulation indicates that supply of critical inputs, including energy or raw materials, as well as food security might affect security or public order concerns. In relation to critical inputs and raw materials, it was indicated in the Proposal to the Framework Regulation, that the Commission launched the European Raw Materials Initiative in 2008 (European Commission, COM(2008) 699 final), which established a list of Critical Raw Materials at the EU level. In 2020 the fourth list of critical raw materials was published by the Commission and it includes 30 materials (European Commission, COM(2020) 474 final), such as Heavy and Light Rare Earth Elements, Cobalt, Lithium, Tungsten or Tantalum.

Fourthly, access to sensitive information, including personal data as well as freedom and pluralism of the media, are also among the sectors that are prone to security and public order concerns under Article 4(1) of the Framework Regulation. Indication of such categories ensures the protection of special personal data regime applicable in the EU in regards to treatment of personal data (under GDPR) (2016) as well as media freedom and pluralism, which are inseparable from freedom, democracy and the rule of law and core basic democratic values on which EU is founded (European Parliament, 2018).

Finally, it should be noted that the list of factors indicated in Article 4(1) of the Framework Regulation concerning sectors or assets that might affect security or public order of a Member State is non-exhaustive (Recital 12 of the Framework Regulation), and it does not preclude a Member State from invoking security or public order concerns over other assets or sectors too.

5.2.2 Criteria pertaining to EU interests and security or public order concerns

Article 8 of the Framework Regulation allows the Commission to raise questions regarding possible effects of foreign direct investment to projects and programmes of Union interest on grounds of security or public order.

Article 8 of the Framework Regulation indicates that the Commission shall be entitled to issue opinion on whether it considers that a foreign direct investment is likely to affect projects and programmes of Union interest. Such projects and programs of Union interest consist of 2 parts: projects and programmes that are indicated in Annex to the Regulation, and which are covered by Union law regarding critical infrastructure, critical technologies or critical inputs which are essential for security or public order (Article 8(3) of the Framework Regulation).

The projects and programmes prescribed in the Annex of the Framework Regulation include: European GNSS programmes (Galileo & EGNOS); Copernicus programme; Horizon 2020 Framework Programme for Research and Innovation, including actions therein relating to Key Enabling Technologies such as artificial intelligence, robotics, semiconductors and cybersecurity; Trans-European Networks for Transport (TEN-T); Trans-European Networks for Energy (TEN-E); Trans-European Networks for Telecommunications; European Defence Industrial Development Programme and Permanent structured cooperation (PESCO).

Critical infrastructure includes 93 European critical infrastructure objects (88 in energy sector, 5 in transport sector) (European Commission, 2019, P. 12-13) and will be clarified in a new legislative action, which is planned for the 4th quarter of 2020. Meanwhile critical technology falls within Horizon 2020 Framework and Key Enabling Technologies indicated in Annex, whereas critical inputs fall within the European Raw Materials Initiative and list of Critical Raw Materials.

5.2.3 Criteria pertaining to investor that might cause security or public order concerns

Article 4(2) of the Framework Regulation indicates that it is not only the sector or asset that is important in assessing possible security and public order risks, but that Member States should also consider 3 criteria related to investor: possible governmental control of foreign investor; previous involvement of the foreign investor in activities affecting security or public order in a Member State; serious risk that the foreign investor engages in illegal or criminal activities.

The governmental control of foreign investor is of utmost importance, because the criteria for the control of foreign investor seem to be broader than attribution criteria used in international law. In international law the "guidance or control" of a person by the state rule is codified in Article 8 of Draft articles on Responsibility of States for Internationally Wrongful Acts (ILC, 2001), which prescribes that actions of a person shall be considered as actions of a State if he acted under direction or control of that state. International tribunals interpreted such "direction or control" as either "effective control test" (ICJ, 1986) or as "overall control test" (International Criminal Tribunal for the Former Yugosloavia, p. 17). Both of these tests are stringent, but the Framework Regulation uses criteria of "indirect control", as well as control through "significant funding", which significantly broadens the notion of control.

It is debatable and not clear yet on what "significant funding" entails, but the Recital 13 of the Framework Regulation notes that it includes subsidies and whether foreign investor is pursuing State-led outward projects or programmes. The most ambitious and far-reaching State-led outward programmes in the world are Chinese: China led initiative of One Belt One Road and state-led policy of Made in China 2025, whose ten key sectors for additional government support (Koleski, 2017) broadly reflects key technologies critical technologies indicated in Article 4(1)(b) of the Framework Regulation. The concern shared by the Commission in 2017 in Reflection Paper on Harnessing Globalisation mentioning investments of state-owned enterprises and predominance of Chinese state-owned enterprises in foreign direct investment activities in the EU, as well as mentioning of state-led outward projects or programmes, singlehandedly directs towards China and Chinese foreign direct investments as a potential source of security and public order concerns.

The criterion of engagement in illegal or criminal activities of foreign investor, without the list or explanation of nature of illegality of activities, also raises questions on the exact contents of such criterion. Neither the text of the Framework Regulation, nor Proposal for the Framework Regulation provide any explanation on the contents of illegal or criminal activity. Every country has a right to prohibit certain activity as illegal and criminalise it or consider certain activity deemed illegal or criminal in the EU as legitimate within its territory. The treatment of Uyghur minority in Xinjiang province of China is debatable between the EU and China, where one sees 're-education camps' as a grieve violation of human rights (European Parliament, 2019), the other sees it as 'vocational education and training' facilities that successfully help to counter terrorism and religious extremism (State Council of the People's Republic of China, 2019). As some major Chinese technology companies employ their respective technologies in Xinjiang, e.g., Hikvision (urban surveillance solutions) or Huawei (public security monitoring through facial recognition, artificial intelligence-based solutions use by Xinjiang police) (OECD, *201, p.* 18) the question is not that clear on how to qualify such foreign companies in regards to engagement in illegal or criminal activities as prescribed in Article 4(2) of the Framework Regulation.

5.3 Criteria on security and public policy limitations under the CJEU practice

Although Framework Regulation provides a guidance on where foreign direct investment may raise security and public policy concerns, the mere existence of potential foreign direct investment in such areas or assets does not justify restriction of foreign investments in these sectors. Any such restriction to foreign investment or investor also constitutes the restriction of one of the fundamental freedoms of the Union – free movement of capital.

Article 63(1) of the TFEU prohibits all restrictions on the movement of capital between member states and between member states and third counties, which includes foreign direct investment. However, Article 65(1)(b) of the TFEU allows the Member States to take measures which are justified on grounds of public policy or public security as long as it does not constitute means of arbitrary discrimination or a disguised restriction on the free movement of capital and payments (Article 65(3) of the TFEU). The same requirement is enshrined in Recital 4 of the Framework Regulation.

According to Article 4(2) of the TEU (2012) and Article 346(1)(a) of the TFEU, matters of national security remain the sole responsibility and exclusive competence of each Member State (CJEU, C-300/11, p. 35). However, although the Member States enjoy exclusive competence in regards to maintenance of public order and the safeguarding of security (CJEU, C-265/95, p. 33), the exceptions to free movement of capital must be interpreted strictly (CJEU, C-463/00, p. 34) and public security may be relied on only if there is a genuine and sufficiently serious threat to a fundamental interest of society (CJEU, C-212/09, p. 83; CJEU, C-54/99, p. 17).

Moreover, the restrictions on capital movement and thus measures adopted after the screening of foreign direct investment, must observe the principle of proportionality, which requires that the measures adopted be appropriate to the objective pursued, and must not go beyond what is necessary to attain that objective (CJEU, C-112/05, p. 73 ; CJEU, C-451/05, p. 82 ; CJEU, C-105/12 to C-107/12, p. 63). Therefore, the Court of Justice does not uphold the restriction on capital movement based on public security if restriction is not suitable to achieve objection intended by such restriction or if the measures in question could have been less restrictive and thus disproportional. For instance, in case *Commission v. Greece* the Court noted that a prior authorisation scheme of holding of more than 10% of the capital of a company operating in the energy sector cannot be regarded as a real and serious enough threat to security of supply, because such scheme produces effects even before a potential threat of decision of the company in regards to interference with the security of supply can materialise (CJEU, C-244/11, paras. 69-71).

Finally, it should be noted that the Commission in its 2020 Guidance (European Commission, 2020) indicated that according to the Case C-446/04 Test claimants in FII Group Litigation (CJEU, 2013, p. 171), the justification and proportionality on restrictions on capital movement to or from non-member countries (such as foreign direct investment) is less strict than for a restriction on capital movements between Member States.

Such opinion and guidance provided by the Commission indicates the encouragement of the Commission towards the Member States to actively employ investment screening measures against foreign investors, especially if they meet the criteria of government control ((in particular though subsidies and managerial control) or risk of illegal activity (Article 4(2) of the Framework Regulation). Furthermore, such guidance of the Commission, especially considering the resemblance of criteria under the Framework Regulation to character of Chinese foreign direct investment (state led programmes and initiatives, government-controlled investors (through equity or especially – finances), similarity of technologies to be nurtured by the EU and additionally supported by Chinese government) indicates that the Framework Regulation is acutely attuned to screening of Chinese foreign direct investment in the EU.

Bibliography

---, “List of screening mechanisms notified by Member States under Framework Regulation”, https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157946.pdf

CJEU (1997), C-265/95, Commission v France, ECLI:EU:C:1997:595

CJEU (2000), C-54/99 Église de scientologie, ECLI:EU:C:2000:124

CJEU (2003), C-463/00, Commission v Spain, ECLI:EU:C:2003:272

CJEU (2006), C-446/04, Test claimants in FII Group Litigation, ECLI:EU:C:2006:774

CJEU (2007), C-112/05, Commission v. Germany, ECLI:EU:C:2007:623

CJEU (2007), C-451/05, ELISA, ECLI:EU:C:2007:594

CJEU (2011), C-212/09, Commission v Portugal, ECLI:EU:C:2011:717

CJEU (2012), C-244/11, Commission v. Greece, ECLI:EU:C:2012:694

CJEU (2013), C-300/11, ZZ v Secretary of State for the Home Department, ECLI:EU:C:2013:363

CJEU (2013), C-105/12 to C-107/12, Essent, ECLI:EU:C:2013:677

Commission Staff Working Document, *Evaluation of Council Directive 2008/114 on identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. SWD(2019) 308 final. 23.7.2019. P. 12-13.

Commission Work Programme 2020. COM(2020) 37 final. 29.1.2020. P.4.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Welcoming Foreign Direct Investment while Protecting Essential Interests. COM(2017) 494 final. 13.9.2017.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. [2008] [OJ L 345].

European Commission (2017), *Reflection Paper on Harnessing Globalisation*. COM(2017) 240 of 10 May 2017

European Commission (2019), *Proposal for a Regulation of the Regulation of the European Parliament and of the Council establishing a framework for screening of foreign direct investments into the European Union*. COM(2017) 487 final, 13 September 2019

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Critical Raw Materials Resilience: Charting a Path towards greater Security and Sustainability.* COM(2020) 474 final. 3 September 2020.

European Commission, Communication from the Commission. *Guidance to the Member States concerning foreign direct investment and free movement of capital from third countries, and the protection of Europe's strategic assets, ahead of the application of Regulation (EU) 2019/452 (FDI Screening Regulation)* (2020) OJ C 99I.

European Commission. Communication from the Commission to the European Parliament and the Council. *The raw materials initiative — meeting our critical needs for growth and jobs in Europe*. COM(2008) 699 final. 4 November 2008.

European Parliament (2018), Resolution of 3 May 2018 on media pluralism and media freedom in the European Union. T8-0204/2018.

European Parliament (2019), Resolution of 19 December 2019 on the situation of the Uyghurs in China. P9_TA(2019)0110.

ICJ (1986), Military and Paramilitary Activities in and Against Nicaragua, Judgement, 1986 I.C.J. Rep. 14, para 86.

ILC, Draft articles on Responsibility of States for Internationally Wrongful Acts. Adopted by the International Law Commission at its fifty-third session, in 2001, and submitted to the General Assembly as a part of the Commission's report covering the work of that session (A/56/10).

International Criminal Tribunal for the Former Yugosloavia, Prosecutor v Tadic, Case No. IT-94-1-A, Para. 117.

Koleski K. (2017), *The 13th Five Year Plan. U.S.-China Economic and Security Review Commission*. Staff Research Report, https://www.uscc.gov/sites/default/files/Research/The%2013th%20Five-Year%20Plan_Final_2.14.17_Updated%20(002).pdf

OECD, FDI Regulatory Restrictiveness Index, https://stats.oecd.org/Index.aspx?datasetcode=FDIINDEX#

Regulation (EC) (2009) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. OJ L 134.

Regulation (EU) (2016) No. 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC. OJ L 119.

Regulation (EU) (2019) No. 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, OJ L 79I.

Rhodium Group and the Mercator Institute for China Studies (2020), *Chinese FDI in Europe: 2019 Update*. Papers on China, April 2020, https://rhg.com/research/chinese-fdi-in-europe-2019-update

State Council of the People‘s Republic of China (2019). White paper. Vocational Education and Training in Xinjiang. 174 August 2019, http://english.www.gov.cn/archive/whitepaper/201908/17/content_WS5d57573cc6d0c6695ff7ed6c.html

The Treaty on European Union (2012), OJ C 326.

Treaty on the Functioning of the European Union (2012), OJ C 326.

Chapter 6 The European Union competence to regulate disinformation

It is widely accepted that disinformation poses a global threat to open and democratic societies, it erodes trust in institutions and in digital and traditional media and harms our democracies by hampering the ability of citizens to take informed decisions, it can polarise debates, create or deepen tensions in society and undermine electoral systems, and have a wider impact on European security (European Commission, 2018). On 15 December 2020 the Council of the EU adopted conclusions which call for further enhanced responses at EU level to counter hybrid threats, including disinformation, and strengthening resilience (Council of the EU, 2020). The Council notes the COVID-19 pandemic makes the EU and its Member States more vulnerable to hybrid threats, including via the intensified spread of disinformation and manipulative interference. The attempts are becoming more sophisticated and are increasing in volume.

The Council acknowledges that the EU approach to addressing disinformation is multidisciplinary and multi-stakeholder (Council of the EU, 2020). Active participation by civil society organisations is a key to offering a comprehensive response to disinformation, researchers, independent fact-checkers, and quality journalism have lately played a vital role in countering the phenomenon (the European Economic and Social Committee, 2020). However, to develop a holistic, systematic and proactive approach to address the phenomena, some Member States have developed legislative framework foreseeing the responsibility of different nature for disinformation acts. The comparative analysis of national legislative initiatives is being performed in the framework of WP4 (T-SHARK program). The preliminary results of the comparative research demonstrate, on the one hand, the increasing tendency to impose responsibility to different actors by law, and, on the other hand, existing disparities in legislative approaches in the different Member States. To complement the above-mentioned analysis, this Chapter discusses whether the EU might harmonise the legislative approaches (non)present in different Member States, thus setting a minimum 'unacceptable' standard of information disorder. To this end, the Chapter reviews the existing EU legislative measures and analyses the extent to which they may be used in countering disinformation.

6.1 The external competence of the EU

To increase cooperation in a variety of fields related to cyber threats, including disinformation, the Member States and the Council took different actions such as the establishment of the Permanent Structured Cooperation (PESCO) in 2017[16]. The European Commission adopted a Joint Framework on Countering Hybrid threats (European Commission, 2016), and established the Rapid Alert System to counter disinformation (EEAS, 2019) under the Common Security and Defence Policy (Art. 42 TEU).

In December 2018, the Commission and the High Representative adopted the Joint Communication on “Action Plan against Disinformation”. The Action Plan responds to the calls of the European Council in June and October 2018 to develop a coordinated response to the challenges in this field (European Commission, 2018). The action plan emphasized four areas of work: improving the capabilities of EU institutions to detect, analyze, and expose disinformation; strengthening coordinated and joint responses to disinformation; mobilizing the private sector to tackle disinformation; and raising awareness and improving societal resilience. It proposed maintaining the

[16] see more : https://pesco.europa.eu/

mandate of the East StratCom Task Force and reviewing the mandates of the Western Balkans and South Task Forces (Pamment James, 2020).

It is true that the measures under the CFSP mandate contribute effectively on the detection and counter fighting of disinformation, as well as common understanding of the importance of the fight against disinformation, however, it does not have the same effect as legal measures that uniformly affect subjects. Therefore, it is important to discuss the possibility of the European Union to approach the disinformation with the legislative measures.

6.2 The shared competence regarding the internal market of the European Union

Article 26(2) of the TFEU establishes the principle of the free movement of services as one of the four main components of the internal market. In this field, the European Union shares the competence with the Member States (Art. 4(2)(a) TFEU), except for Union's exclusive competence only to establish the competition rules necessary for the functioning of the internal market (Art. 3(1)(b) TFEU).

There are some documents introduced on this basis of Article 4(2)(a) TFEU relevant to the prevention and fight of disinformation. The Audio-visual Media Services (AVMS) Directive, adopted in 2010 and amended in 2018, regulates broadcasting of AVMS (radio, television and concerned Internet services), and the Directive on electronic commerce (or E-Commerce Directive) of 2000, regulating the liability of hosting and related services.

6.2.1 AVMS Directive: derogations from the Country-of-Origin principle

In 2010, the EU adopted a first regulation to codify the provisions, regulations and practices, regarding the AVSM, in order to ensure the fair competition and the proper functioning of the internal market (Preamble of the Directive). The AVMS Directive have been amended in 2018, to include, in addition to the "classic" AVMS such as television, the "video-sharing platform service" which does not have an editorial responsibility, such as YouTube (Article 1 of AVMSD). The amendment of 2018 aimed at considering the new technology development. However, it does not include the platform providers which content is not devoted to provide programs or user-generated videos. Therefore, other social media, such as Facebook or Twitter, are excluded from the scope of this directive (Article 1). Indeed, the AVMS Directive designates "television-like services", similar to mass media and by consequence cannot apply to Social Media and other platform providers, which are more individual user's content (European Parliament Report, 2019), and provide a variety of services or type of content going beyond the audio-visual.

The *Country of Origin (COO) principle*, established in Art. 2 is central to the Directive. The country-of-origin principle means "that each EU Member State is responsible for ensuring the compliance with the law of audiovisual media services transmitted by media service providers under its jurisdiction" (Volman, 2018).

Article 2 of the Directive requires the Member States "to ensure freedom of reception" and does not allow to "restrict retransmissions on their territory of audio-visual media services from other Member States for reasons which fall within the fields coordinated by this Directive". Notwithstanding the application of the country-of-origin principle, Member States may still take measures that restrict freedom of movement of television broadcasting, but only under the conditions and following the procedure laid down in this Directive. However, the Court of Justice has consistently held that any restriction on the freedom to provide services, such as any derogation from a fundamental principle of the Treaty, must be interpreted restrictively (CJEU, C-355/98, p. 28; CJEU, C-348/96, p. 23).

There are two sets of derogations from the Country-of-origin principle establishing in Article 3 of the Directive. The first group of derogations targets the protections of accepted community interests, i.e., tackling hate and violence, and protecting minors. They are related to the "manifest, serious and grave" acts of incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter (Art. 6(a)), impairment of

the physical, mental or moral development of minors (Art. 6a(1)) or a serious and grave risk of prejudice to public health (Art. 3(2) of the Directive).

Any derogation made under the above mentioned grounds should satisfy the following conditions set out in the same Article: (a) during the previous 12 months, the media service provider has on at least 2 prior occasions already performed one or more instances of conduct described above; (b) the Member State concerned *has notified the media service provider*, the Member State having jurisdiction over that provider and the Commission in writing of the alleged infringements and of the proportionate measures it intends to take should any such infringement occur again; (c) the Member State concerned has respected the right of defence of the media service provider and, in particular, has given that provided the opportunity to express its views on the alleged infringements; and (d) consultations with the Member State having jurisdiction over the media service provider and the Commission have not resulted in an amicable settlement within one month of the Commission's receipt of the notification mentioned in point b). The Commission takes a decision on whether those measures are compatible with Union law. Where the Commission decides that those measures are not compatible with Union law, it shall require the Member State concerned to put an end to the measures in question as a matter of urgency.

The second group of derogations targets security interests. A Member State may provisionally derogate from the *Country of Origin Principle* where an audio-visual media service provided by a media service provider under the jurisdiction of another Member State "manifestly, seriously and gravely" infringes the prohibition of public provocation to commit a terrorist offence as set out in Article 5 of Directive (EU) 2017/541 (Art. 6(1)(b)) or "prejudices or presents a serious and grave risk of prejudice to public security, including the safeguarding of national security and defence".

The Directive as all other EU legal acts, mentioned above does not define the notion of the public or national security. However, it is interesting to mention, that public security is presented as a wide concept encompassing national security and defence. In the countries where disinformation is accepted as a crime in certain circumstances, the restriction of retransmissions on their territory of audio-visual media services by a country may be based on this ground. However, the COO principle does not accept a general derogation in case of disinformation unless the State can demonstrate the serious and grave risk to national security.

This derogation is subject to the following conditions: (a) during the previous 12 months the conduct referred to in the first subparagraph occurred at least on one prior occasion; and (b) the Member State concerned has notified the media service provider, the Member State having jurisdiction over that provider and the Commission in writing of the alleged infringement and of the proportionate measures it intends to take should any such infringement occur again. The Member State concerned shall respect the rights of defence of the media service provider concerned and, in particular, give the opportunity to express its views on the alleged infringements.

The third possibility to limit *Country of Origin Principle* is to follow the rules established in Article 4(2) of the Directive preventing the phenomenon of "forum shopping". Third States might find ways to circumvent strict national legislation by using EU internal market and settling in another Member States with the less strict legislation. Z. Kokoly observes that the revised version of the AVMS Directive "extends the power of the Member States to trigger a circumvention procedure based on reasonable cause rather than the former requirement to prove intention of circumvention by the provider, a previously seemingly impossible task for national regulating authorities" (Kokoly, 2019, p. 45). Z. Kokoly also points out that the anti-circumvention procedure has retained its dual structure, comprising two phases: a non-binding consultation phase (Art. 4(2)) and the anti-circumvention procedure itself, which can result in the adoption of appropriate measures against the media service providers concerned (Art.4(3)-(5)) (Kokoly, 2019, p. 59). One of the key novelties in the text of Directive 2018/1808 is the extension of the anti-circumvention procedure to all media content in order to comprise not only linear audio-visual media broadcasts but also non-linear media services (Kokoly, 2019, p. 59).

Thus, Art. 4(3) of the Directive envisages that if the service is "wholly or mostly" directed towards its territory and the State of destination adopted more detailed or stricter rules of general public interest (Art. 4(2)), the State of destination can request the State of origin to address any problems identified,

expecting sincere and swift cooperation aiming for “mutually satisfactory solution”. Since the state of origin has the jurisdiction over the media service provider, it must request it to comply with the rules of general public interest in question and inform the requesting Member State about the steps and results of the anti-circumvention procedure. The revised Directive “reiterates the necessity of regularly informing the requesting Member State of the steps taken to address the problems identified, but it also includes a new obligation of explaining the reasons where a solution could not be found” (Kokoly, 2019, p. 60).

If the results appear to be unsatisfactory, and the media service providers chooses to establish itself in other States to avoid the jurisdiction of a particular State, the State of destination can adopt the appropriate measures against the media service provider (Art. 4(3)). Here it is important to mention that the most significant changes regarding the anti-circumvention procedure in the revised AVMS Directive is lifting the burden of proving intent, since proving intentional circumvention of law by requesting Member States has been a constant issue of debate (Kokoly, 2019, p. 60).

The Member states may definitely use this clause to fight disinformation. In the case *Baltic Media Alliance Ltd v Lietuvos radijo ir televizijos komisija* of 2019 (CJEU, C-622/17, p. 80) the CJEU accepted that disinformation could pursue, in general, a public policy objective. The case concerned the decision of 18 May 2016, which had been taken on the ground that a program broadcast on the channel NTV Mir Lithuania contained false information which incited hostility and hatred based on nationality against the Baltic countries concerning the collaboration of Lithuanians and Latvians in connection with the Holocaust and the allegedly nationalistic and neo-Nazi internal policies of the Baltic countries, policies which were said to be a threat to the Russian national minority living in those countries (CJEU, C-622/17, p. 79). According to the Lithuanian Radio and Television Commission the program was addressed in a targeted manner to the Russian-speaking minority in Lithuania and aimed, by the use of various propaganda techniques, to influence negatively and suggestively the opinion of that social group relating to the internal and external policies of the Republic of Lithuania, the Republic of Estonia and the Republic of Latvia, to accentuate the divisions and polarisation of society, and to emphasise the tension in the Eastern European region created by Western countries and the Russian Federation’s role of victim (CJEU, C-622/17, p. 79). The Lithuanian government applied the rules of Article 4 accordingly, since they were proving that the service was exclusively directed towards its territory.

Therefore, Member States retain the possibility to restrict the application of the country-of-origin principle in case of disinformation, even though disinformation is not specifically mentioned like hate speech or protection of minors. If the Member States could come up with the common definition of disinformation, it could in theory appear in the text of the Directive among other ‘evils’ to fight against and thus could gain more visibility among media service providers. One the other hand, the current regulation leaves more room for manoeuvre, since in case of disinformation the Members state may choose between two procedures. It is true that the derogations are subject to strict procedural conditions, which restricts the ability to act quickly and efficiently. In order to limit the dissemination of disinformation coming from a media service based in another Member State, seriousness of the risk against national security has to be demonstrated by a state of reception, which might be difficult in case of one piece of disinformation.

6.2.2 The E-commerce Directive: obligation to remove illegal content

The Directive on Electronic Commerce of 2000 is also relevant in the context of disinformation. The objective of this Directive is to create a legal framework to ensure the free movement of information society services between Member States and not to harmonise the field of criminal law as such (Preamble, para. 8). At the time of adoption, the measure was believed as constituting the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information (Preamble, para. 40).

The E-commerce Directive includes the immunity regarding “hosting content” as long as the service provider did not have knowledge of illegal activity. When the service provider has the knowledge of the existence of illegal content, it must “act expeditiously” to remove the information (Article 14 (1) (b)). However, the Directive does not allow the member states to impose a general obligation on

providers to monitor the information, which they transmit, or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity (Art. 15 (1)). Members States are able to establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities (Art.15 (2)).

There is no definition of “illegal content” or “illegal activity” in the Directive. As a result, the EU and national law must define it. In its communication the European Commission indicated some content, e.g., hate speech and incitement to violence, terrorism and harmful content, which is considered to be illegal (European Commission, 2016). No surprise, disinformation is not in the list, since the recognising of different forms of disinformation as an illegal activity is in a different stage of development. “This presents a gap for other forms of harmful content, as both misinformation and disinformation are not necessarily unlawful” (Shattock, 2020).

Therefore, the use E-Commerce directive as one of the tools to fight disinformation varies from country to country. Since there is no common agreement of the Members states of what disinformation is and it is not mentioned as a separate category next to illegal content, even if disinformation presents a harmful content it will not provoke the obligations under Article 15.

6.2.3 The Code of Good Practice on Disinformation: lack of common terminology

Adopted on October 2018, the EU Code of Practice on Disinformation (2018) is a code enclosing various non-binding commitments to tackle disinformation. It is understood as a dissemination of information from which we can verify whether they are false or misleading, and which are created presented and spread for “profit or with the intention of deceiving the public” (preamble) while they are "likely to cause public harm" (preamble) in the sense of "threats to political and democratic policymaking processes and to public goods, such as the protection of the health of Union citizens, the environment or security” (preamble). During the assessment of the Code of Practice on Disinformation, legal issues are still not addressed and remain.

As it is voluntarily based, it requires the subscription to this Code. In June 2020, TikTok joined the other platforms, such as Google, Facebook, Twitter, Microsoft and Mozilla. They took a certain number of commitments but out of them, only efforts “commercially reasonable” are expected to be met. Indeed, the rationale behind is the self-regulation (European Commission, 2020). Among the main aspects, the Commission referred to the scrutiny of ad placements, transparency of political and issue-based advertising and integrity of service.

As mentioned above regarding commitments that are variable depending on the stakeholders, the other legal issue relates to the procedural aspect regarding the definition, the scope but also the application and hence the monitoring of the Code (European Commission, 2020, p. 10). Accordingly, stakeholders that signed the Code committed themselves to the redaction of an annual report of their works. Furthermore, the signatories also committed to use a third objective body to evaluate their accomplishment against the commitments taken.

Also, there is no “dedicated, user-friendly and uniform procedure available” on all platforms for users to flag possible disinformation cases and be adequately informed about the “outcome of their actions”, while one of the priorities is to “empower the consumers” (European Commission, 2020, p. 10).

The COVID-19 crisis confirmed the need for clarification of additional concepts, a better glossary for terms used to avoid a variety of false, misleading or even manipulative behaviour or information. The *Infodemic* spread its outbreak from healthcare systems to minorities (ethnic or religious groups). It linked itself with hate speech, which eventually led to an “exacerbation of the social polarisation in the EU” (European Commission, 2020, p. 12).

The Code uses the definition of “disinformation” set out in the April 2018 Communication and consistently used by the Commission in various statements.

Disinformation is understood as verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policy- making processes as well

as public goods such as the protection of EU citizens' health, the environment or security. Disinformation does not include reporting errors, satire and parody, or clearly identified partisan news and commentary" (Communication, 2018, p. 3-4).

However, the COVID-19 "infodemic" has highlighted the need to further clarify additional concepts and differentiate more precisely between various forms of false or misleading content and manipulative behaviour intended to amplify its dissemination online in order to enable the framing of appropriate responses by the platforms and other relevant stakeholders (European Commission, 2020, p. 12). The Reports points out again at the need for a better scoping of the disinformation phenomenon through the articulation of certain adjacent concepts, in particular "misinformation" and "influence operations", as well as number of other operational terms (European Commision, 2020, p. 12-13). The lack of common understandings of the scope of fundamental concepts and of uniform definitions of key operational terms inhibits the effective implementation of measures by the signatories and impedes the monitoring, evaluation and comparison of the Code's implementation and effectiveness across platforms and Member States. It may also inhibit further take up of the Code insofar as potential signatories may be uncertain about the scope of commitments, they would be undertaking by signing up to the Code (European Commission, p. 13).

Bibliography

CJEU, Baltic Media Alliance Ltd v Lietuvos radijo ir televizijos komisija, Case C-622/17, 4 July 2019, para. 80.

CJEU, C-348/96, Calfa, ECR I-11

CJEU, C-355/98, Commission v Belgium, ECR I-1221

Council of the EU (2020), Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic, https://data.consilium.europa.eu/doc/document/ST-14064-2020-INIT/en/pdf

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ L 95, 15.4.2010, p. 1–24

EEAS (2019), Factsheet: Rapid Alert System, https://eeas.europa.eu/headquarters/headQuarters-homepage/59644/factsheet-rapid-alert-system_en

EU Code of Practice on Disinformation (2018), https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

European Commission (2016), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM/2016/0288 final

European Commission (2016), Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats a European Union response, JOIN/2016/018 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

European Commission (2018), Action Plan on disinformation: Commission contribution to the European Council (13-14 December 2018), https://ec.europa.eu/commission/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en

European Commission (2018), Tackling online disinformation: a European Approach, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236&from=en

European Commission (2020), Commission staff working document, Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement, Brussels, 10.9.2020, SWD(2020) 180 final

European Parliament (2019), Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States.

Kokoly, Z. (2019), The Anti-Circumvention Procedure in the Audiovisual Media Services Directive, ActA Univ. SApientiAe, LegAL StUdieS, 8, 1 (2019) 43–64, http://acta.sapientia.ro/acta-legal/C8-1/legal81-03.pdf

Pamment James (2020), The EU's Role in Fighting Disinformation: Taking Back the Initiative, https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286

Shattock, Ethan (2020), Is it time for Europe to reassess internet intermediary liability in light of coronavirus misinformation?, https://europeanlawblog.eu/2020/04/20/is-it-time-for-europe-to-reassess-internet-intermediary-liability-in-light-of-coronavirus-misinformation/

Volman Lucas (2018), "Is the cornerstone loose? Critical analysis of the functioning of the 'country of origin' principle in the Audiovisual Media Services Directive, taking into account the rapid changes in the audiovisual industry and the recent challenges brought by Brexit", https://www.bai.ie/media/sites/2/2018/09/BAI-Media-Content-Regulation-Essay-Lucas-Volman.pdf

Chapter 7 Summary and Conclusion

Despite some attempts to interpret the concept of national security in soft EU law, there is no clear definition of what is to be understood as 'national security' in EU legislation. So far, such criteria of national security have become clear: activities by intelligence and security services are generally accepted as falling under the national security exemption; also, national security cannot be considered as defence, state security, public security, the prevention, investigation, detection and prosecution of criminal offences, etc. And there are no clear criteria to distinguish between these categories. The concept of national security is regulated in individual states, but it is not very specific. Attempts to define it very specifically seem to go unnoticed. At present there is no uniform national definition in the laws of the EU countries.

Neither the relevant provisions of EU law, nor the CJEUs/ECtHR case law offers a clear definition of what 'national security' is. Moreover, the EU and its Member States use various rather similar notions related to security without defining them: internal security, national security, state security, public security and defence should all be distinguished. It is considered that any cyber threat analysis and prediction system should comply with national requirements related to the protection of national security. And in order to use such kind of systems acting also outside one EU country, greater harmonization of national security concepts should be initiated.

Regulation establishing a framework for the screening of foreign direct investments into the Union is a legislative solution of the European Union to address the risk of FDI affecting security and public order of Member States or the Union. Regulation is clear that the decision on the screening of foreign direct investment on the basis of national security or essential security interests lies within individual Member States. That includes determination for the Member States on what exactly constitutes security and public order for each individual member state. As substantial number of EU Member States do not have any instruments on screening of foreign direct investment, the Framework Regulation provides a guidance on what sectors, assets or investor related aspects might raise such concerns. However, the Regulation is clear that any decision based on the screening of foreign direct investment has still meet the requirements applicable to restriction of free movement of capital, i.e., that it has to be justified, proportionate and appropriate. Nevertheless, the Commission's opinion and guidance provided in 2020 demonstrates the encouragement for the Member States to actively employ investment screening measures against foreign investors, especially if they meet the criteria of government control (in particular though subsidies and managerial control) or risk of illegal activity.

Under AVMS Directive Member States retain the possibility to restrict the application of the country-of-origin principle in case of disinformation, even though disinformation is not specifically mentioned like hate speech or protection of minors. If the Member States could come up with the common definition of disinformation, it could in theory appear in the text of the AVMS Directive among other evils to fight against and thus not only could gain more visibility among media service providers but also unificate the practice.

The use of E-Commerce directive as one of the tools to fight disinformation also varies from country to country. Since there is no common agreement of the Members states of what disinformation is and it is not mentioned as a separate category next to illegal content, even if disinformation presents a harmful content it will not provoke the obligations under Article 15.

Finding the right balance between the interests of different stakeholders is notoriously difficult and that even if the actors from industry and law enforcement are aware of the issue of social impacts it remains difficult to make sure that all values at stake are protected in the same way. Policy makers (at least at the European level) became aware of this challenge a few years ago when they developed (or rather adopted) the concept of "responsible research and innovation" to ensure that research carried out with EU funding reflects the societal consequences of their own actions. It is also obvious that the social groups affected by cybersecurity measures and the range of impacts can vary greatly and depend strongly on the concrete use cases, so that no concrete instructions for action can be given apart from very general guidelines. As a way out of this conflict, we have pro-

posed a process to enable stakeholders (especially the researchers themselves) to think systematically about the possible impacts of the technology they are developing in different dimensions. This process takes up the idea of technology readiness, which is widely used in (EU) research funding, and complements it with the concept of societal readiness.

We have proposed a reflection tool to improve the societal readiness level (SRL), that envisages four so-called gates over the duration of the research and development process, i.e. times when certain issues should be discussed by scientists and research managers, ideally with the involvement of likely users and stakeholders. Although each technology development must find its own answers, there are already extensive catalogues of possible issues and also extensive approaches to address identified undesirable consequences or conflicts.

We have proposed to adopt the tool for the specifics of cyber security. It is then planned to test the tool together with the SPARTA programmes in the remaining time of the project. Since we foresee that there will be some hesitation against the additional effort, the success of this exercise will depend heavily on the commitment of the WP and task leaders involved.

With a view to the future development of cybersecurity in Europe, we have put forward some initial ideas on how to incorporate the consideration of ethical, legal and societal aspects into the emerging organisations and their mandate. The proposed reflection process could, for example, become a standard procedure to be used by EU-funded cybersecurity projects. However, this also means that the necessary resources would have to be earmarked and the necessary expertise would have to be maintained, e.g. by the ECCC.

Chapter 8 List of Abbreviations

Abbreviation	Translation
CERT	Computer Emergency Responson Team
CJEU	Court of Justice of European Union
CVD	Coordinated Vulnerability Disclosure
ECHR	European Convention on human rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
ICJ	International Court of Justice
ILC	International Law Commission
NSA	US National Security Agency
RRI	Responsible Research and Innovation
TEU	Treaty of the European Union
TFEU	Treaty of the Functioning of the European Union

Chapter 9 Appendix 1. Questionnaire (GDPR related issues)

WP2: Mapping of specific SPARTA Programs' related problems

This document includes the challenges arising from Programs 6 (HAII-T- and Program 7 (SAFAIR). With regard to the description of these programs, the question listed below relate to the General Data Protection Regulation (GDPR). We have chosen not to differentiate issues by program in order to take as cross-cutting an approach as possible.

I. Effectiveness

- Quality of the content given by the data subject
    - How to define security requirements in a precise but comprehensive manner for citizens?
    - Should we give more information to the data subject than what is required by the GDPR in order to ensure a transparent processing and to obtain the consent?
    - What information should be given to the data subject to understand the system's functioning?
    - How to provide the information to obtain an informed consent?

II. Necessity and proportionality

- Anonymization and pseudonymization in cybersecurity innovation?
- How to prevent re-identification issues?
- How should we manage the minimization and proportionality principles set by the GDPR with the need to have the most data as possible "to feed" and design efficient algorithms in order to avoid bias? What are the major obstacles in the collection of personal data to avoid algorithmic bias?

III. Accountability

- Who will be responsible in case of data breaches? The users? The creators of the algorithms? The one who collects the datasets? Etc
- Should the manufacturers be also responsible?
- It is important that, in the use of cloud computing services, the data controller keep the control over the client of cloud computing services. What mandatory obligations should be given by the data controller?

IV. Fairness

- What criteria are needed to assess fairness in cybersecurity innovation?

- What data sharing model between operators working in security? How to distribute the roles of the different stakeholders?
- Availability and security: What balance must be struck between the confidentiality requirements, the availability requirements and the right to erasure granted to the data subjects?
- How to adopt a user-centric approach in the context of cybersecurity innovation?
- Does the right to the portability of personal data imply interoperability? If so, how can it be exercised in a cybersecurity context? If not, should it be made mandatory?
- How can we always guarantee the trust of users while ensuring that they are aware of the potential risks?
- How to integrate the human intervention in cybersecurity innovation?
- How to manage the use of personal data for cybersecurity innovation with the right to be left alone?
- Transparency and algorithm: Should the transparency obligation of the data controller relate to the algorithm (open source) or to the processing of the personal data?

Chapter 10 Appendix 2. Mapping ELSA of the Programs

WP	Tasks	Partner	Focus	ELSA
WP4 T-SHARK		L3CE	T4.2 and T4.3: handling complex cybersecurity threats T4.4: exchanging of threat intelligence information T4.5: Analysis of the national legal framework governing the approach towards disinformation	**GDPR specific issues:** 1) *Legal basis - National Security Exemption in the context of GDPR* 2) Monitoring process 3) Differentiation between collection and access of the data **Specific issues:** *1) Legislative power of the EU to prevent disinformation* 2) Wide scope of cyber security threats, however, still geographically narrow legal response 3) The need for the integration of different types of data from various actors 4) No commonly agreed definition for politically motivated information disorder 5) Influence operations vs. freedom of expression 6) No national archive 7) Foreign investment screening 8) Security and Public Order criterion under EU Investment Framework Regulation 9) SRL (Societal Readiness Assessment), ect.
WP5 CAPE	T5.2 Vertical 1	FTS	Car platooning: automation of transport of goods through a platoon of vehicles.	**GDPR specific issues:** possible sharing of personal data. Data share between the cars is mostly anonymous with identification of the vehicles through keys, data on velocity and direction. Data shared: number of plates, materials transported, data from the scanning of surroundings (by sensors not camera). This data is not used to address the technological aspect but might be used for business purposes. So, it seems that there is no exchange of

WP	Tasks	Partner	Focus	ELSA
				personal data between cars, only between owner and service provider. **Specific issues:** related to the accountability of a manufacturer A) Balancing the no-fault insurance with traffic (and product) liability B) The extent of manufacturer ‘s obligation to prevent cybersecurity attack in the scenario „security to safety“ (under Regulation (EU) 2019/2144)
WP5 CAPE	T5.3 Vertical 2	CINI	E-Governance: development of an Electronic Identity Card Authentication with one-time password generation or via mobile	**GDPR related issues:** Regarding GDPR claim that no data is stored or use according to GDPR requirement: only use the ID code, which is transmitted to the service provider. The service provider might have more information based on this ID code.
WP5 CAPE	T5.1	FBK	Develop tools to find solution to the issues that might appear during the building process of supply chain software (attacks, malware, etc.)	**GDPR related issues:** non identified at the moment **Specific issues:** 1) Licensing of all the tools developed to deal with liability problem 2) *Responsible disclose of security vulnerabilities* – ethical or legal? Some countries have some regulation or legislative proposals on disclosure of vulnerabilities
WP6 HAII-T		BUT	Develop a foundation for secure-by-design Intelligent Infrastructure T1 to T4 focused on security aspects	In T6.5 GDPR aspect, see below.
WP6 HAII-T	T6.5	UTARTU	Creation of a tool to analyze GDPR compliance in business processes Evaluate GDPR compliance of a business process model and compare with different models	**GDPR related issues:** Still in development phase, might need assistance regarding the GDPR *Operationalization/automation of GDPR not only the compliance check but also the other two modules on DPIA and data breaches would be of interest* *Could be used for the car platooning business model*

Chapter 11 Appendix 3. Questions for Gate 1 to Gate 4 (tables)

Gate 1	Anticipate	Reflect	Include	Respond
Public Engagement	- How will you ensure that you maintain good relations with your stakeholders? - At which phases in the project will stakeholder involvement have the most crucial impact, and why?[b] -How early in the project do you plan to involve potential stakeholders?[g] -Who will be the primary users/beneficiaries of the project, and could this change? -Who will not benefit from the project? - How will different stakeholders benefit from your project?	-Have you considered alternative definitions of and approaches to the problem at stake?[c] Have relevant stakeholders been involved in defining the research problem? -Who are the relevant stakeholders of your project?[e]	-What actions will be taken to ensure diversity in terms of gender, nationality, ethnicity, class, age, etc. among the involved stakeholders?[c] -What actions will be taken to involve all potentially relevant stakeholders including researchers, representatives from industry, policy-makers and civil-society actors in the project?[h]	- Is it possible to change problem formulation or project design in response to changing stakeholder viewpoints or unforeseen ethical issues arising throughout the project?

Gate 1	Anticipate	Reflect	Include	Respond
Open Access	-What aspects of the project do you plan to make open access? [b] -What can you do to ensure that all project partners comply with your open-access strategy? -Could pre-registration ensure transparency and openness in this project?	-How do the partner organizations involved in the project approach open access, and how could you align potentially diverging approaches?[b] -What are the potential barriers to making your data, coding and publications open access and how could these barriers be addressed? -Do you have valid reasons for not preregistering you research?	-What can be done to make proceedings and the final results of your project easily accessible and intelligible to a diverse set of stakeholders?[d] -With whom do you plan to share the results of your work?[b]	
Science Education	-Will the project contribute new knowledge of relevance for science education, and how? -Could your project benefit from involving citizens in data collection and analysis, and how?	-Can RRI perspectives be integrated into the training and supervision of project staff, and how? - What would it take to better accommodate citizens interested in contributing to your work, and how? - How do you plan to communicate the uncertainty of your research?	- Which stakeholders will take part in the project's education and training activities, and why?[b] -Will your education and communication activities be tailored to specific stakeholder groups, and which?[b]	
Gender	-How may your project contribute to improve gender balance in academia? -Could the outcomes of this project benefit from incorporating a gender dimension into research content, and how?	-What are the barriers to gender balance among researchers and leaders in this project and how can these be addressed?? -What are the possible gender and sex dimensions of the problem at stake?	-What can be done to ensure gender balance among researchers and leaders in this project? -What can be done to ensure gender diversity among research subjects?[c]	

Gate 1	Anticipate	Reflect	Include	Respond
Ethics	-Why should this project be done?[a] -What ethical issues could your project potentially give rise to?[b] - To what extent will you be able to predict the long-term societal outcomes of the project?[a]	- What actions should be taken to ensure research integrity and compliance with ethical standards in the project?[b] - Does your project involve any risks of negative impacts, and which?	-Who will be involved in identifying the ethical issues and possible solutions to these issues in your project, and how?[b] - What actions will be taken to ensure diverse perspectives on the potential ethical issues arising in your project?	

Table 3: Questions for Gate 1 – Research Design and Problem Formulation. Source: Nielsen et al. (2017)

The questions were adopted or adapted from existing work: a= Jirotka et al. (2017); b= https://www.rri-tools.eu/self-reflection-tool (2018); c= (Kupper, Klaassen, Rijnen, Vermeulen, and Broerse 2015); d= Andersen (2017); e= Stahl et al. (2015); f= Stilgoe, Owen, and Macnaghten (2013); g= Callon, Lascoumes, and Barthe (2011); h= Kupper, Klaassen, Rijnen, Vermeulen, Woertman, et al. (2015), CEN (2017).

Gate 2	Anticipate	Reflect	Include	Respond
Public Engagement	-Will any potentially relevant beneficiaries or end-users be missed by the selected method for data collection? -How might the project benefit from involving stakeholders in identifying proper methods for data collection and empirical testing?	- Have you engaged in dialogue with all relevant stakeholders so far, and how? - Who have been involved in designing the data collection / testing? - How has the nature and purpose of the project been communicated to external stakeholders?[f] -Did the data collection give rise to new consideration about potentially relevant stakeholders, and which?	-How will you ensure that all stakeholders feel empowered to voice their opinion?[c] - how will you ensure that all relevant stakeholders have theinformation they need to engage in a meaningful dialogue about proper procedures for data collection and testing?[g]	-Is it possible to change procedures for implementation, data collection and testing in response to ethical issues or stakeholder viewpoints in this phase?

Gate 2	Anticipate	Reflect	Include	Respond
Open Access	-How may the selected methods for data collection and testing best be documented to ensure transparency and allow for replication and knowledge transfer?	- How do you plan to document your methods for data collection / testing in an intelligible and transparent way? -What are the potential barriers to making documentations of data collection and testing publicly accessible (e.g. intellectual property rights, competing interests)	-With whom will you share potential documentations of data collection and testing?[b]	
Science Education	-Will the project contribute new methods and techniques of relevance for other researchers and practitioners?	-Will it be possible for interested citizens to contribute to the collection of data, and how? -How can you ensure that interested stakeholders understand the purpose and approaches of the project?	-Which stakeholders are taking part in your education activities, and why these?[b] - If your project contributes new methods and techniques of relevance for other researchers and practitioners, how do you plan to support the education of these groups?	

Gate 2	Anticipate	Reflect	Include	Respond
Gender	-Will the selected methods for data collection / testing, and sample-size allow for nuanced analysis of possible gender- and sex-related differences and similarities?	- Have gender and sex related issues been taken into consideration in the selected methods for data collection and testing, and how? -What is the sex composition of the subjects included in the collected sample? Will it be possible to change procedures for data collection and testing to allow for nuanced gender and sex analysis?	- How do you plan to identify participants that do not identify as men or women (e.g. non-binary or gender fluid subject) in the data collection?	
Ethics	- Can you imagine possible scenarios of misuse associated with the methods and data you are using?[i]	-Is the planned research methodology ethically acceptable, including aspects related to data collection and data storage?[a] -Does your data collection require informed consent from the participants? - Does your project involve any risks of breach of confidentiality and what might they be?	-Who have been involved in identifying the ethics-related issues to be considered in the data collection?[b] - Have certain groups of potential participants been excluded from the data collection due to ethical concerns, and how may this limit your analysis?	

Table 4: Questions for Gate 2 – Implementation, Data Collection & Testing. Source: Nielsen et al. (2017)

The questions were adopted or adapted from existing work: a= Jirotka et al. (2017); b= https://www.rri-tools.eu/self-reflection-tool (2018); c= (Kupper, Klaassen, Rijnen, Vermeulen, and Broerse 2015); d= Andersen (2017); e= Stahl et al. (2015); f= Stilgoe, Owen, and Macnaghten (2013); g= Callon, Lascoumes, and Barthe (2011); h= Kupper, Klaassen, Rijnen, Vermeulen, Woertman, et al. (2015), CEN (2017).

Gate 3	Anticipate	Reflect	Include	Respond
Public Engagement	-Which stakeholders may benefit from your results, and how?[f] -Which stakeholders may not benefit from your results, and why?[f]	-Who have been involved in data-analysis and evaluation, and why? -Did the data-analysis and evaluation give rise to new considerations about potentially relevant stakeholders, and which?	-How will you ensure that all stakeholders have the information they need to engage in a meaningful dialogue about data analysis and evaluation? -Have the results been discussed with different types of stakeholders to allow for alternative interpretations?	- Is it possible to change procedures for data analysis and evaluation of project results in response to ethical issues or stakeholder viewpoints in this phase?
Open Access	-How may the data analysis and evaluation best be documented to ensure transparency and allow for replication and knowledge transfer?	-Did you document your data analysis / evaluation in an intelligible and transparent way, and how? -What are the potential barriers to making code-scripts and documentation of the full analysis publicly accessible (e.g. intellectual property rights, competing interests, confidentiality etc.)	-With whom will you share the documentation of your analysis and evaluation?[b]	

Gate 3	Anticipate	Reflect	Include	Respond
Science Education	-Will the project contribute new analytical and evaluative methods of relevance for other researchers and practitioners, and how do you plan to support this? -What do people not participating in the project (teachers, students museums, Civil society organizations) need to know about the data analysis and evaluation of project results to learn about/ engage with the outcomes of your work?	-How may interested citizens contribute to your data analysis?	-What types of training do you provide for citizens to contribute to your data analysis?	
Gender	-How may your findings impact gender norms and gender relations in society?	- Has your data analysis focused attention to possible gender- and sex-related differences and similarities, and how?	-Have you analysed possible interactions between gender and sex and other sociodemographic variables such as class, ethnicity, race, nationality and age, and how?	
Ethics	-Can you think about beneficial applications of your results beyond the original scope of your work? -Can you imagine possible scenarios of misuse?[i] -Could your findings be misinterpreted, and how?	-What ethics-related issues are involved in your data analysis? -What types of sensitivity analysis have been used to test the robustness of your methods and results? -	- Did your analysis devote attention to possible variations across sub-groups of participants, and how?	

Table 5: Questions for Gate 3 – Data analysis and evaluation. Source: Nielsen et al. (2017)

The questions were adopted or adapted from existing work: a= Jirotka et al. (2017); b= https://www.rri-tools.eu/self-reflection-tool (2018); c= (Kupper, Klaassen, Rijnen, Vermeulen, and Broerse 2015); d= Andersen (2017); e= Stahl et al. (2015); f= Stilgoe, Owen, and Macnaghten

(2013); g= Callon, Lascoumes, and Barthe (2011); h= Kupper, Klaassen, Rijnen, Vermeulen, Woertman, et al. (2015), CEN (2017).

Gate 4	Anticipate	Reflect	Include	Respond
Public Engagement	-How can your stakeholder engagement experiences inform furture engagement activities in your research area?	-To what extent does your dissemination plan address the relevant user and beneficiaries of the project? [d]	-Is your dissemination plan be tailored to target the needs and characteristics of specific stakeholder groups?[b]	- Is it possible to change your launching and dissemination activities in response to needs and concerns of societal actors?
Open Access	-Who will be responsible for maintenance and storage of the open-access information after the project ends, and for how long? -Could the data collected as part of this project be useful for other research purposes, and which? -Could the information made open access be misused, and how?	-Is the open access information accompanied by clear and transparent documentation of data editing, statistical procedures and analytical decisions made through-out the project? - Is the information made open access accompanied by clear specifications on data structure and variable descriptions to allow for replications or new research purposes?	-Will all open access information be available in English? - Is licensed software required to benefit from your open acess information? -Will publications hidden behind paywalls be accompanied by freely accessible pre-print copies?	
Science Education	-How may your results contribute to the public interest in and understanding of science? -How may the results of this project be used in the education of future generations of researchers and engineers?	-How will your results be communicated to the broader public?	-Will the results of your project be available in other languages than English?	

Gate 4	Anticipate	Reflect	Include	Respond
Gender	-What impact do expect your project will have on gender equality?	-What is the gender balance among the authors on the peer reviewed papers resulting from this project? -Will both women and men be taking roles as leading authors? -Are the results reported by sex and gender in your publications, and how? What can be done to help support the future career of both men and women junior scholars in the project?	[To be populated] How will you communicate your results in a way that does not reinforce gender stereotypes?	
Ethics	- Can you imagine possible scenarios where the outcomes of the project may be misrepresented or misconstrued in the public debate?	- How will you brief the participating research subjects about the project results? What can be done to ensure that your results are not misrepresented or misinterpreted in the public debate?	[To be populated] Do you plan to involve possible stakeholders in discussions about the ethical implications of your project results?	

Table 6: Questions for Gate 4 – Launching and dissemination. Source: Nielsen et al. (2017)

The questions were adopted or adapted from existing work: a= Jirotka et al. (2017); b= https://www.rri-tools.eu/self-reflection-tool (2018); c= (Kupper, Klaassen, Rijnen, Vermeulen, and Broerse 2015); d= Andersen (2017); e= Stahl et al. (2015); f= Stilgoe, Owen, and Macnaghten (2013); g= Callon, Lascoumes, and Barthe (2011); h= Kupper, Klaassen, Rijnen, Vermeulen, Woertman, et al. (2015), CEN (2017).

Chapter 12 Appendix 4. Table of Implementation of CVD policies at national level in Europe, based on CEPS' own contribution

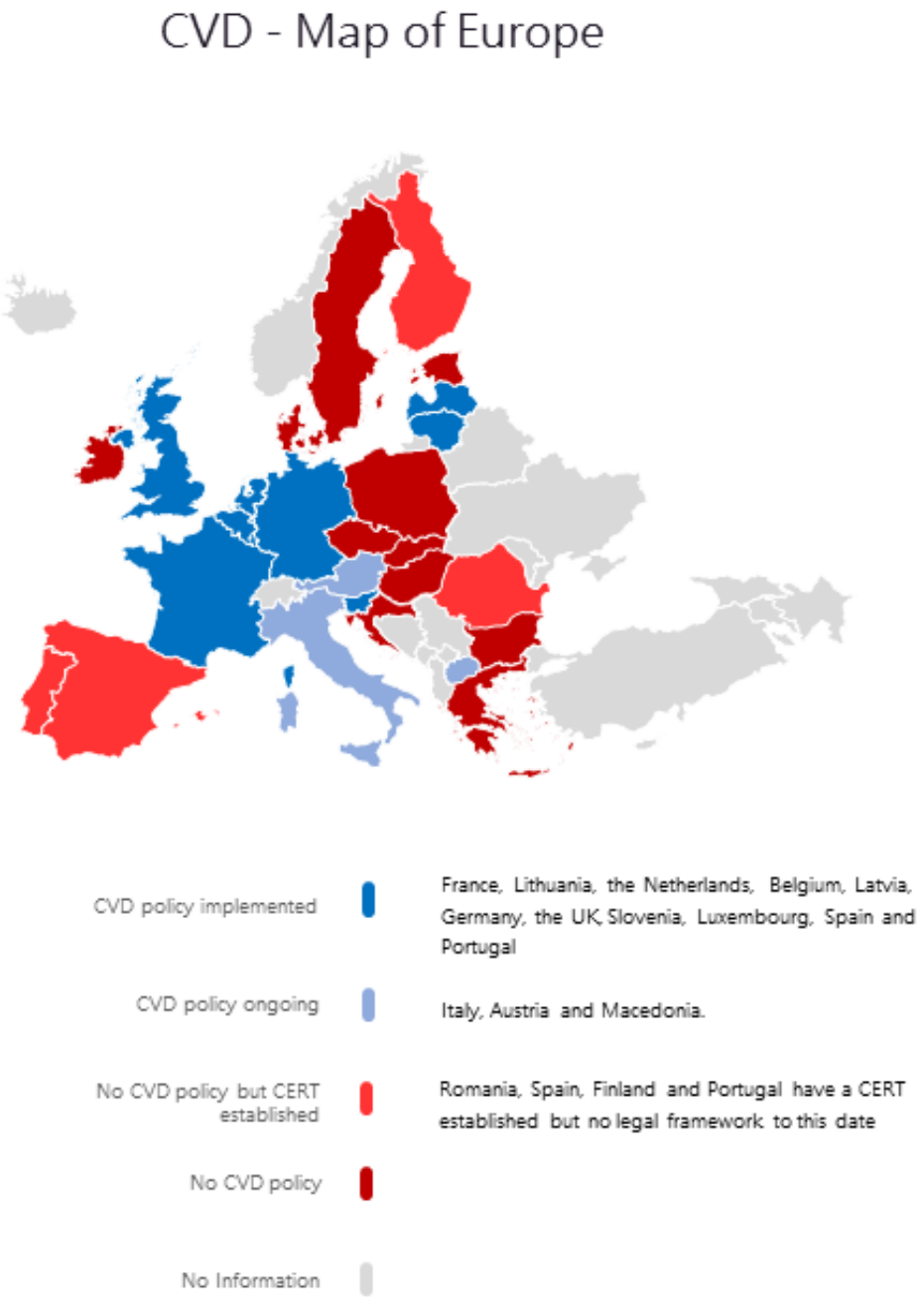
Source: adapted from CEPS, 2018 and updated by authors (CEPS, 2018)

CVD policy at national level	Status	Country
YES	CVD policy implemented : partial protection of the researcher (CEPS, 2018)	France
	CVD policy implemented : full protection of the researcher	Lithuania
	CVD policy implemented : full protection of the researcher (CEPS, 2018)	Netherlands
	CVD policy implemented : partial protection of the researcher	Belgium
	CVD policy implemented : very detailed scope, full protection of the researcher (except if known criminal)	Germany
	CVD policy implemented : partial protection of the researcher	Latvia
	CVD policy implemented : the researcher is solely responsible for compliance with law. Complying with this policy is not intended to provide with any protection if breaching the law, nor does this policy give permission to act in any manner that is inconsistent with the law as it applies to the researcher or the NCSC.	UK
	CVD policy implemented : the vulnerability must be unknown and severe enough to be considered as eligible for a mention in the Hall of Fame of GOVCERT.LU	Luxembourg
	CVD policy implemented : acts under this Responsible Disclosure Policy should be limited to conducting tests to identify potential vulnerabilities, and sharing this information with relevant authority. Partial protection for researcher. Hall of Fame system	Slovenia

ONGOING	Italian Manifesto to be presented to the Public Sector Organisations	Italy
	Ongoing discussions on this issue (CEPS, 2018)	Austria
		Macedonia

NO		Czech Republic
		Finland
	CERT established but no legal framework yet	Romania
		Spain
		Portugal
		Finland
	No activity (CEPS, 2018)	Bulgaria Croatia Cyprus Ireland Estonia Poland Sweden

Chapter 13 Appendix 5. Map of current CVD policies in Europe



Source: adapted from CEPS, 2018 and updated by authors

Chapter 14 Appendix 6. Map of current CVD policies in Europe

Questionnaire

"On Coordinated Vulnerability Disclosure national measures"

Comparison Study

Coordinating institution of the study: Mykolas Romeris University (MRU – Lithuania)

Deadline for submitting the information: April 2021

The answers to the questions will be used to develop the comparative analysis of existing national measures regarding Coordinated Vulnerability Disclosure (hereinafter CVD). The term CVD designates the practice of reporting a vulnerability to a coordinating authority – CERTs (Computer Emergency Response Team). A vulnerability is understood as a breach or a cybersecurity threat to an IT system. The research seeks to address the comparison of the legal responsibility regime of the one's finding (researcher or finder) the vulnerability among different Member States, at the moment, using the most recent available data.

Topic		*Yes/No (if relevant)*	*Please provide details to your answer.*
1. Identification	Please indicate your country		

2. National Measures regarding CVD	Which of the following measures have been implemented officially in your country?		
	Legislation (please indicate the full name in English and in original language)		
	Date of adoption		
	Areas of legislation		
	To whom is the legislation applicable?		
	Please provide the e-links to the legislation (if possible, to English version)		

	Non legislative acts (please indicate the full name in English and in original language)		
3. National Coordinating Institution	Which institution is responsible for coordinating vulnerabilities disclosure? (e.g.: https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network)		
	Please provide the e-links to the national institution (if possible, to English version)		
4. Procedural aspects	Is there a formalized procedure for reporting the vulnerability?		
	If yes, please provide the references to the legislation (e-links and provision(s) of the legal act(s), If possible, to English version)		
5. Responsibility of the Researcher (finder)	Is there any specific legal regime for the Researcher's responsibility when looking for vulnerabilities?		
	If yes, what type of responsibility may apply? (civil, criminal, both)		
	If yes, please provide the references to the legislation (e-links and provision(s) of the legal act(s), if possible, to English version)		
Legal protection of the researcher (finder)	Is confidentiality of the researcher (finder) guaranteed?		
	Is legal protection of the researcher conditioned to certain criteria?		
	Is legal protection of the researcher extended to his/her family?		
	Please provide the references to the legislation (e-links and provision(s) of the legal act(s), If possible, to English version)		
Participation in CVD programme	Incentives for the Researcher**:** is there any policy for motivating potential researchers to participate in CVDs programmes (yes/no)		
	If yes, what is the nature of the measure (financial, academic, etc.)?		

Discussion on legislative measures	If there are no formal legislative measures yet in place, are there any above-mentioned measures currently under discussion?		
	Which measures?		
	What is the stage of discussion? (intent date of adoption a legal measure, etc.)		
	Please provide the reference as e-links, if possible		