SPARTA

D2.1

Ethical, legal and societal aspects

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-830892 / D2.1 / V1.0
Work package contributing to the deliverable	WP2
Due date	January 2019 – M12
Actual submission date	3rd February, 2020

Responsible organisation	UNamur
Editor	Manon Knockaert
Dissemination level	PU
Revision	V1.0

Abstract	After attempting to provide an initial definition of the concept of cybersecurity, this deliverable focuses on determining the ethical values (mainly security, privacy, fairness, accountability) and legal imperatives (fundamental rights and protection of personal data) relevant in the context of cybersecurity. Finally, the public attitudes towards privacy and security values is studied.
Keywords	Privacy, Data Protection, Ethics, Cybersecurity, Fairness

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

Editor

Manon Knockaert (UNamur)

Contributors (ordered according to beneficiary numbers)

Manon Knockaert, Jean-Marc Van Gyseghem (UNamur)

Michael Friedewald, Ralf Lindner (FHG)

Reviewers (ordered according to beneficiary numbers)

Vincent Roca (INRIA)

Rashel Talukder (PPBW)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

From a legal and political point of view, the notion of ‘cybersecurity’ seems to be intrinsically linked to the preservation of the integrity, confidentiality and availability of the information. This conception is also reflected in the General Data Protection Regulation. Indeed, Recital 49, article 5 and article 32 link the notion of incidents to cyberattacks that affect the availability, authenticity, integrity and confidentiality of personal data.

Four “value clusters” that include a range of values might be relevant in the context of cybersecurity namely security, privacy, fairness and accountability.

Security as a value refers to objective and subjective conditions. The objective conditions refer to the risk management and loss prevention. The latter does no longer focus on dangers and hazards and replaces them by risks, which have an (un)certainty to occur. They are based on the assumption that risks cannot totally be prevented and damages and losses will occur anyway. The focus of this approach is no longer directed towards the source of the damage, but towards the management of the effects with the goal to minimise the adverse effects for those affected.

In its subjective acceptation, the security refers to a personal feeling. This means that subjective security is individually different and context-dependant.

Cybersecurity is an imperative that must be placed at the service of fundamental rights and must ensure their effectiveness, in particular the right to privacy, the right to the protection of personal data, the right to freedom of expression and the right to non-discrimination. The law requires a risk-based approach and an appropriate level of security regarding the risks, the probability that these risks will occur and seriousness of the risks for the citizens.

Privacy is a broader concept than personal data protection and encompasses privacy of behaviour and action, privacy of communication, privacy of thought and feelings, privacy of location and space and privacy of association. The use of such multi-dimensional concept of privacy is useful, since new technologies, especially in the area of cybersecurity technologies, often do not influence such dimensions at all, which for example focus on data protection. Rather, privacy of location, privacy of behaviour and privacy of thoughts and feeling are currently threatened through the use of soft biometrics, smart video-surveillance and of kinds of AI based security applications.

In order to address privacy and data protection issues in the cybersecurity context, key questions are raised:

- What is the expected and actual level of transparency?
- How much data and what data need to be gathered? What data should be accessible to whom? For how long should these data be stored?
- What balance must be struck between the confidentiality requirements, the availability requirements and the right to erasure granted to the data subjects?
- Who will be responsible in case of data breaches? How can PETs be integrated in a more global reflection on the management of personal data and the risks generated by the activities and processing of the data controller?
- What data sharing model is expected between stakeholders wording the cybersecurity area?

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

In its common acceptance, the notion of cybersecurity is understood as "*the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this*"[1].

However, this definition seems critical for two main reasons. Firstly, ENISA points out the lack of precision[2] and secondly, it does not fit with the European Commission's understanding.

Indeed, in its Joint communication entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", the European Union states that: "*freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role*"[3]. And cybersecurity is defined as "*the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*"[4].

Security seems thus to be defined by its objectives, namely the preservation of networks and infrastructures from any attacks that could have as consequences to affect the availability, integrity and confidentiality of the information. Following this approach, the European Commission establishes five principles for the cybersecurity in the European Union[5]:

- The EU's core values apply as much in the digital as in the physical world;
- Protecting fundamental rights, freedom of expression, personal data and privacy;
- Access for all;
- Democratic and efficient multi-stakeholder governance;
- A shared responsibility between all stakeholders-public and private sector- to ensure security.

After the publication of its strategy by the European Commission, the Cybersecurity Coordination Group (CSCG)[6] released a white paper called "Recommendations for a Strategy on European Cyber Security Standardisation"[7]. Several recommendations are made. We can highlight the Recommendation 2:

[1] This definition is from The Oxford English Dictionary. On this point, see also ENISA, Definition of Cybersecurity: Gaps and overlaps in standardisation, December 2015, v.1.0.

[2] For a reasoned criticism, see ENISA, Definition of Cybersecurity: Gaps and overlaps in standardisation, December 2015, v.1.0, p. 10.

[3] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final, p. 2.

[4] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final, p. 3.

[5] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final, pp. 3-4.

[6] This group gathers the three official European Standardisation Organisations (CEN, CENELEC and ETSI).

[7] CEN_CENELEC/ETSI- Cyber Security Coordination Group, Recommendations for a Strategy on European Cyber Security Standardisation", v. 01.08.

"*The EC should establish a clear and common understanding of the scope of Cyber Security, based on an initiative the CSCG plans to launch to clarify the key terms and definitions used in the standardisation of and communication related to Cyber Security within the European Union.*

To establish clear understanding, the CSCG recommends that the European Commission should harmonise its usage of the key terms "Cyber Security", "NIS" and "cybercrime" across the EU on the basis of existing definitions. Official communications currently use all three terms without distinguishing between them, which risks them being interpreted differently in different EU Member States (or languages). The CSCG recommends that the European Commission should not limit its clarification to definitions but should also establish an agreed understanding of the interdependencies and relationships between the three areas in question. The CSCG also recommends that the Commission should establish and enforce a suitable governance model for the three areas, with special emphasis on avoiding working in silos on topics that are inherently intertwined"[8].

Later, in 2015, the European Union Agency for Cybersecurity (ENISA) released its document entitled "Definition of Cybersecurity: Gaps and overlaps in standardisation"[9]. A state of the art concerning the understanding and the various definitions in the European Union is made. From this document, it transpires that the notion of cybersecurity depends on:

- The activity area;
- What we want to preserve/protection: communications, operations or information;
- The various organisations active in the field.

The following figure[10] and table[11] provided by ENISA illustrates the various meaning of the notion of "cybersecurity".

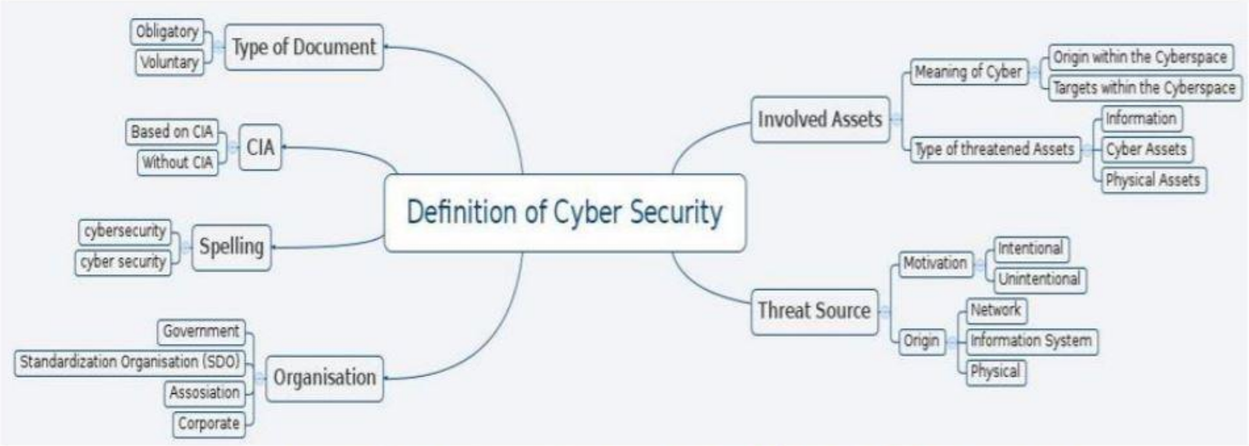
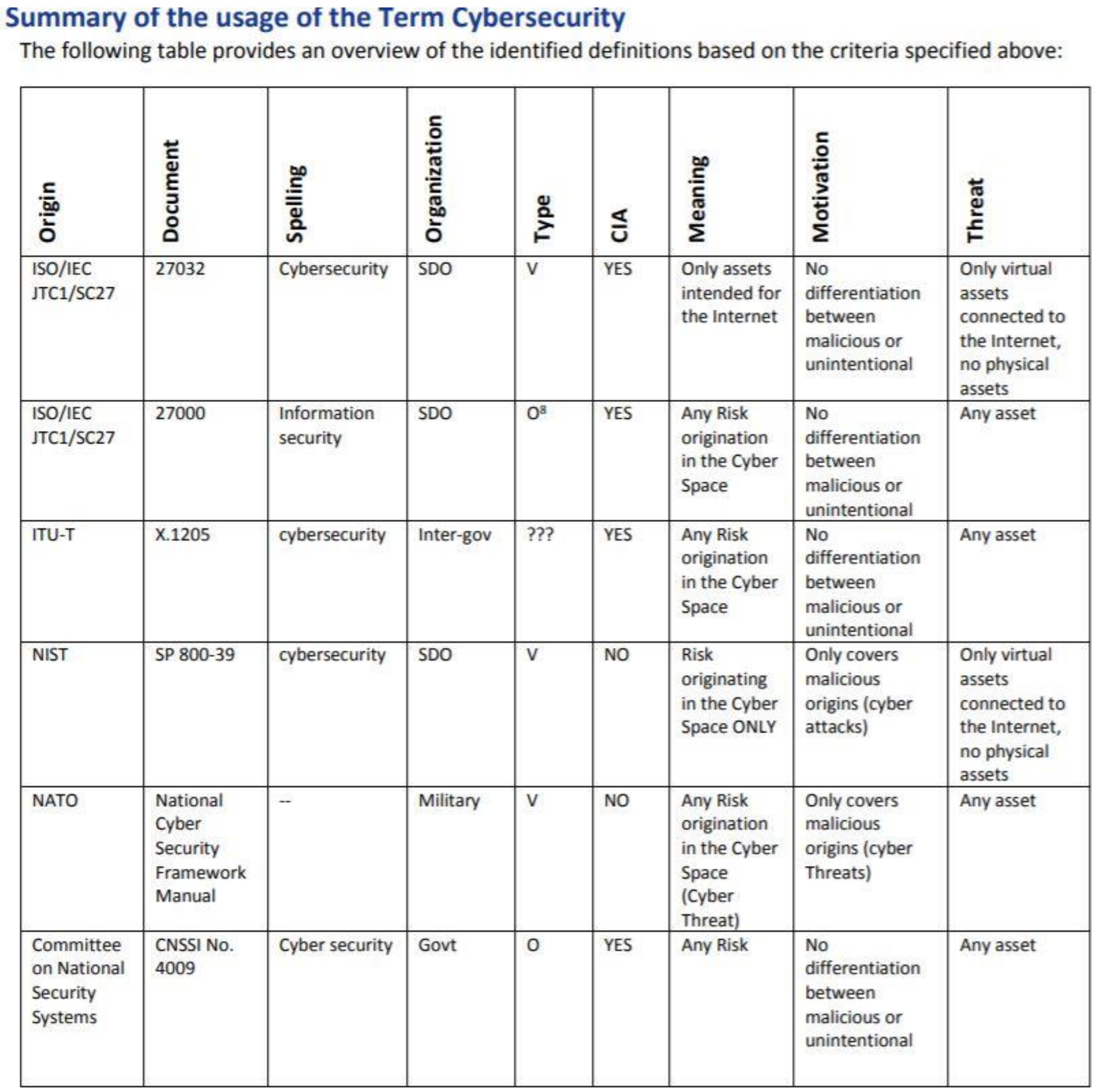


Figure 1: Components constituting the definition of Cybersecurity (ENISA)

[8] CEN_CENELEC/ETSI- Cyber Security Coordination Group, Recommendations for a Strategy on European Cyber Security Standardisation", v. 01.08, p. 11.
[9] ENISA, Definition of Cybersecurity: Gaps and overlaps in standardisation, December 2015, v.1.0.
[10] ENISA, Definition of Cybersecurity: Gaps and overlaps in standardisation, December 2015, v.1.0, p. 13.
[11] ENISA, Definition of Cybersecurity: Gaps and overlaps in standardisation, December 2015, v.1.0, p. 19.



Summary of the usage of the Term Cybersecurity

The following table provides an overview of the identified definitions based on the criteria specified above:

Origin	Document	Spelling	Organization	Type	CIA	Meaning	Motivation	Threat
ISO/IEC JTC1/SC27	27032	Cybersecurity	SDO	V	YES	Only assets intended for the Internet	No differentiation between malicious or unintentional	Only virtual assets connected to the Internet, no physical assets
ISO/IEC JTC1/SC27	27000	Information security	SDO	O[8]	YES	Any Risk origination in the Cyber Space	No differentiation between malicious or unintentional	Any asset
ITU-T	X.1205	cybersecurity	Inter-gov	???	YES	Any Risk origination in the Cyber Space	No differentiation between malicious or unintentional	Any asset
NIST	SP 800-39	cybersecurity	SDO	V	NO	Risk originating in the Cyber Space ONLY	Only covers malicious origins (cyber attacks)	Only virtual assets connected to the Internet, no physical assets
NATO	National Cyber Security Framework Manual	--	Military	V	NO	Any Risk origination in the Cyber Space (Cyber Threat)	Only covers malicious origins (cyber Threats)	Any asset
Committee on National Security Systems	CNSSI No. 4009	Cyber security	Govt	O	YES	Any Risk	No differentiation between malicious or unintentional	Any asset

Table 1: Summary of the usage of the Term Cybersecurity (ENISA)

After observing that it was impossible to reach a single signification covering the various situations and the various national interpretations, ENISA calls for a contextual definition based on what is relevant in a concrete situation[12].

Finally, in 2017, the European Commission delivered its second joint communication entitled “Resilience, Deterrence and Defence: Building strong cybersecurity for EU”[13]. However, this paper does not clarify the concept of cybersecurity as its main objective is to establish the Commission's next strategies to strengthen the security of products and services within the Union[14].

[12] ENISA, Definition of Cybersecurity: Gaps and overlaps in standardisation, December 2015, v.1.0, p. 28.

[13] European Commission, “Resilience, Deterrence and Defence; Building strong cybersecurity for the EU”, 13.9.2017; JOIN(2017) 450 final.

[14] Namely strengthening ENISA, the European certification framework, implementing the NIS Directive, resilience through rapid emergency response, a cybersecurity competence network with a European Cybersecurity Research and Competence Centre, building a strong EU cyber skills base and promoting cyber hygiene and awareness,

As a first conclusion, it seems that the notion of cybersecurity is intrinsically linked to the preservation of the integrity, confidentiality and availability of the information. This conception is also reflected in the General Data Protection Regulation[15]. Indeed, Recital 49, article 5 and article 32 link the notion of incidents to cyberattacks that affect the availability, authenticity, integrity and confidentiality of personal data.

Moreover, the NIS Directive[16] defines the notion of security of network and information system's as: "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems"[17].

Finally, the recent Regulation 2019/881[18] (knows as "Cybersecurity Act") defines cybersecurity as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats"[19].

Based on the previous developments and literature[20], the following figure represents the components of the notion of cybersecurity.

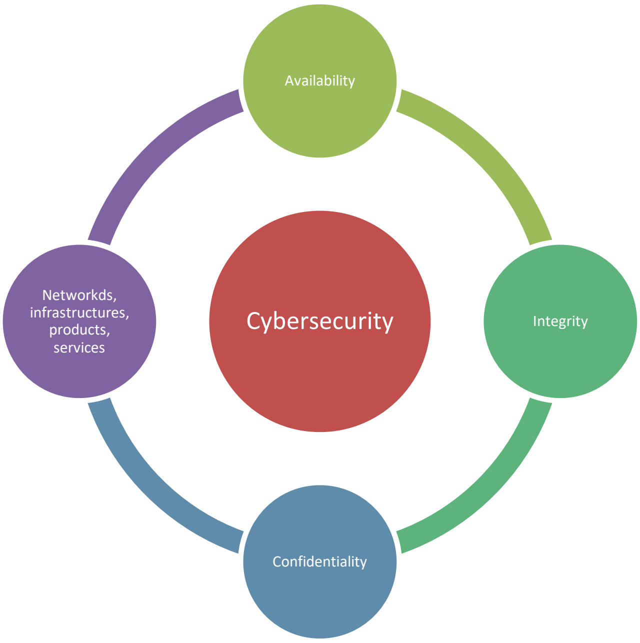


Figure 2: Components of the notion of cybersecurity

[15] 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 (GDPR), L 119/1, O.J., 4.5.2016.

[16] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, L 194/1, O.J., 19.7.2016 ("NIS Directive").

[17] Article 4.2 of the NIS Directive.

[18] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, L 151/15, O.J., 7.6.2019. ("Cybersecurity Act").

[19] Article 2.1 of the Cybersecurity Act.

[20] See notably D. ORLANDO and P. DEWITTE, "The 'by design' turn in EU cybersecurity law: Emergence, challenges and ways forward", *in Security and Law*, A. VEDDER, J. SCHROERS, CH. DECUING and P. VALCKE (eds.), Cambridge, Intersentia, 2019.

Chapter 2 Ethical issues in cybersecurity

People live by a variety of implicit and explicit rules based on cultural, religious and philosophical concepts and beliefs. These rules allow individuals to determine whether their behaviour is right or wrong. The concepts and beliefs, called values, that make up the rules have been formulated, generalized and codified by cultures or groups over a long period of time. The main purpose of the value-based rules is to regulate the behaviour of members of that culture or group in order to create happiness and contentment for all group members. A value can be important for the individual in itself (intrinsic value) or it can help to generates intrinsic value (instrumental value).

Ethics is dedicated to the study of right and wrong in human behaviour. Johnson et al. (2003) for instance defines ethics as a set of theories "that provide general rules or principles to be used in making moral decisions and, unlike ordinary intuitions, provides a justification for those rules". When dealing with ethical issues, the first question obviously is what constitutes an ethical issue. For this purpose, we distinguish three types of ethical issues:

1. Ethical issues may occur when human values (taken broadly) are violated.
2. Ethical issues may also occur in situations when the outcome of actions in support of one value conflict with another.
3. Ethical issues may finally occur when new (types of) problems arise for which no moral principles (taken broadly) exist, or when it is not clear which principles to apply to particular cases.

According to Christen et al. (2016) there is a large number of potential moral values in general, the number of values that they consider important for cybersecurity, however, is limited. Yaghmaei et al. (2017) suggest using the following set of cybersecurity-related values:

Values investigated in ethical research	“European” Values	Values investigated in empirical research	Values referred to in the technical domain
Autonomy Beneficence Dignity Equality Fairness Freedom Justice Privacy Responsibility	Human Dignity Freedom Democracy Equality Non-discrimination The rule of law Respect for human rights Pluralism Tolerance Justice Solidarity Protection of EU citizens	Privacy Security Trust ***Data protection goals:*** Availability Confidentiality Integrity Intervenability Transparency Unlinkability	Privacy Fairness Autonomy ***Practical goals of cybersecurity technology:*** Availability Confidentiality Integrity

Table 2: Cybersecurity-related values (Yaghmaei et al. 2017, p. 8)

To create more order in this multiplicity of relevant values in cybersecurity, van de Poel (2019) has suggested to define "value clusters" that include a range of values of similar moral concerns and respond to somewhat similar ethically problematic situations. For the sake of simplicity we will make use of the four clusters, namely security, privacy, fairness and accountability.

2.1 Core values

2.1.1 Security

It seems obvious that "security" is a central value in the field of cybersecurity, as cybersecurity can be regarded as a subcategory of security. In chapter 1 we have tried to delineate the term cybersecurity in its political meaning. Security as a value, however, has multiple dimensions. As a matter of fact, researchers have stated that the "multidimensional nature of security results in both a society and industry that has no clear understanding of a definition for the concept of security. Moreover, the current concepts of security are so broad as to be impracticable" (Brooks 2009).

2.1.1.1 Conceptualisation of security

A first important distinction that has to be made is that the state of security refers to objective and subjective conditions. Lucia Zedner, a professor of criminal justice in Oxford, writes: "*The objective state of absolute security implies a condition of being without threat, which, even if it could be achieved today, always remains liable to negation by new threats tomorrow. Although we may aspire to the state of security, it makes sense to recognize that its perfect attainment is unachievable, not least since security is predicated on the continuing presence of that which threatens it. Understood this way, security is the condition of 'being protected from threats' -- whether through their neutralization, through avoidance, or through non-exposure to risk*" (Zedner 2009, p. 14).

This is a conventional view in which risk and uncertainty has a negative connotation and is regarded as a threat that individuals or society as a whole has to eliminate (or at least reduce as far as possible with the available resources). This leads to a security orientation in society; risks are only taken because people assume they can be calculated and controlled.

In recent years this view has partly been replaced by that of risk management and loss prevention. The latter does no longer focus on dangers and hazards and replaces them by risks, which have an (un)certainty to occur. They are based on the assumption that risks cannot totally be prevented and damages and losses will occur anyway. The focus of this approach is no longer directed towards the source of the damage but towards the management of the effects with the goal to minimise the adverse effects for those affected.

Apart from the objective absence of harmful events the term security is also used to describe our subjective security feeling. Zedner continues: "*Security is also used to refer to a second state, namely the subjective sense we have of our own safety. In this second sense, security is all in the mind: though of course our subjective sense of safety derives in part from material and social conditions. The subjective state of security as tranquillity or freedom from care has long historic roots that are traceable to the Latin* securitas *and the German* Sicherheitsgefühl*, both of which denote the feeling of being secure*" (Zedner 2009, p. 16).

Psychological stress research indicates that there are multiple stages of cognitive appraisal on the way from objective to subjective security. An individual first categorises a situation as irrelevant, beneficial, or stressful. In the case of a stressful event it is then evaluated as either a harm/loss, a threat, or a challenge. Each of these categories evokes different emotional responses, i.e. such diverse feelings as sadness, fear or excitement. During a secondary appraisal the individual now evaluates his or her coping resources and options to deal with the situation. Consequently, the same situation can be evaluated very differently depending on different factors. For instance, the same event is more likely to be evaluated as irrelevant when it is far away while it might be seen as a threat in immediate vicinity. This means that subjective security is always individually different and context-dependent. As a working definition we refer to the European Committee on Standardisation working group 161:

> "Security is the condition (perceived or confirmed) of an individual, a community, and organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity,

> terrorism or other deliberate or hostile acts, disasters (natural and man-made)" (cited in Martí Sempere 2011, p. 248).

This definition can be combined with the risk management approach, so that security is characterised by (1) a low probability of the occurrence of damaging events and/or (2) a high probability that an effective risk management can largely avoid or compensate the damaging consequences of event and (3) the avoidance of negative side effects of the risk management.

2.1.1.2 Views on and dimensions of security

Security has a different meaning depending on the group of stakeholders and it has many dimensions that depend from the context, ranging from social security to technologically secure systems. While we do not want to discuss "security" for all these contexts here (cf. Lagazio 2012), it is useful to give a systematic overview. This allows classifying and characterizing "cybersecurity" correctly in this spectrum.

On the one hand one has to distinguish the problem area, being the main asset or value that is secured. This ranges from physical security to political security, socio-economic security, cultural security, and environmental security to cybersecurity. Here we focus exclusively on cybersecurity.

On the other side one there are different actors that frame problems and impacts in a slightly different way. For instance, cyber-attacks can be viewed from a state point of view as something the state needs to protect citizens and companies against; as a matter of increasing social resilience from a societal point of view; and for individuals will see cyber-attacks in the context of safeguarding their personal assets.

In the following list cybersecurity is characterized according to these dimensions:

- International organizations (international security)
  - Protection of information and information systems across national borders and social divisions
  - Protecting and promoting secure access, use and development of information across national borders.
  - Protection of identity and information produced by a global and diverse humanity.
- States (national security)
  - Protection of national information and information systems
  - Ensuring and promoting safe access, use and development of national information
  - Protection of identity and information produced by citizens
- Companies and other organisations (corporate security)
  - Protection of corporate information and information systems
  - Assuring compliance with information law, international standards, best practices and appropriate state-of-the-art technology.
  - Ensuring and promoting safe access, use and development of corporate information
  - Protection of identity and information produced by employees and customers
- Civil society (social security)
  - Protection of society's information and information systems
  - Ensuring and promoting safe access, use and development of social information
  - Protection of identity and information produced by social groups and civilians
- Citizens (individual security)
  - Protection of your own information, information system, identity and privacy
  - Secure access, use and development of own information and identity

As security is considered as one of the fundamental human needs, there is a good reason to consider some dimensions of security, in particular individual, physical security as intrinsic values. Social and corporate security can be at least considered as instrumental values. This is more difficult with more collective forms of security, such as national and international security that are more than the other dimensions linked to questions of power.

2.1.2 Privacy[21]

2.1.2.1 Conceptualisation of privacy

When talking about values in the context of cybersecurity, privacy is often mentioned as a central value, and it is often assumed that security is only possible at the cost of a loss of privacy. As is the case of security, however, there is no general agreement on how to exactly define and operationalise the value of privacy. Nevertheless, there is some common understanding about the different components of privacy: Privacy can be understood as a social value and public good as well as an individual value (see e.g. Regan 1995; Kasper 2007; Gutwirth 2002; Fairfield et al. 2015). The two dominating concepts, however, are *access theories* and *control theories*.

Access theories - dating back to the foundational publication by Warren et al. (1890) -- usually define privacy through access (or inaccessibility) to a person or his/her data respectively. Anita Allen, for instance, argues that "in perfect privacy no one has any information about [person] X, no one pays any attention to X, and no one has physical access to X" (Allen 1988, p. 15). Such access-oriented definitions of privacy, however, received criticism for confusing privacy with unwanted isolation or loneliness. This refers to the aspect of control, where the individual decides whether a situation is considered as "private" or as unintended solitude. In the information society where a plethora of information is collected, transferred and processed the question of pure access also appears increasingly irrelevant.

Concepts of privacy that follow this argumentation are called *control theories*. Already in 1967 Alan Westin has described privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967, p. 7). The idea that privacy is the ability of the individual to control the terms under which personal information is acquired and used has been endorsed by a broad community of scholars (e.g. Fried 1970; Rössler 2005) and has also found expression in the prevailing legal opinion. One example is the fundamental right to informational self-determination defined by the German Constitutional Court, which "in principle guarantees the power of individuals to make their own decisions as regards the disclosure and use of their personal data" (*Census Act* 1983).

Although many authors have recognized privacy as a social good the dominant view on privacy (and data protection) is an individual right one, assuming that each human being is enjoying the value of privacy (Rössler 2005; Steeves 2009). In particular control theories therefore problematise the question how to guarantee to individuals an effective control over their own data.

2.1.2.2 Privacy as an intrinsic and instrumental value

Since we all have different preferences for privacy and use it as a commodity, we ought to think about how much we should ask for in return for our privacy. In making this decision, it is useful to think about what we value about privacy. Some researchers have argued that privacy is valuable in and of itself (intrinsic value), while others see privacy mainly as an instrumental value that allows us to reach our intrinsic values.

[21] Following van de Poel (2019) we consider notions such as autonomy, human dignity, identity, personhood, liberty, anonymity and confidentiality as part of ”privacy”.

Mordini (in Gutwirth et al. 2011) points out that the concept of the private origins from biology and therefore has an intrinsic value. Research on territoriality and overcrowding has shown that virtually all animals seek periods of individual seclusion of small-group intimacy, because continuous overcrowding can function as an intensifier of stressful condition (Ford et al. 1979). At the same time humans have developed to the highest degree the ability of empathy, a capacity to reproduce the emotional and mental patterns of others, what makes them not only in their rationale to survive but also in their very neurological structure dependent on other human beings. That is why isolation can be much more pathological than overcrowding (Haney 2003).

Arguing from a psychoanalytic point of view, Mordini also shows that Sigmund Freud understood the private sphere as involving a dichotomy between "civilized society, which demands a good conduct" of its citizens, and instinctual behaviour of the individual. Since society has allowed itself to be misled into tightening the moral standards to the greatest possible degree, the creation of the private realm serves above all as a safety valve for all of the instinctual constraints weighing heavily upon the individual (Freud 1957).

A majority of researchers argue in a liberal tradition, that privacy protects the individual interest in autonomy and moral personhood since it creates a space around the individuals where they can think, judge and act in a self-determined way and free of social or political pressure. In this way privacy enables us to live in ethical manner but is not necessarily itself intrinsically valuable. In this tradition of thinking it is necessary to protect individuals from interference by the state (and other powerful organizations) and to limit the acquisition, possession and spread of information about him. Such an undisturbed space around individuals and the free thinking it enables also has societal benefits (e.g. reducing surreptitious manipulation in elections, allowing citizens to question laws of a country). This shows that privacy is not only in the individual's but also in the society's interest. This thinking has also been dominating the legal discourse about privacy and data protection – though it has been criticised of the last decades (Rössler 2005; Mokrosinska 2017).

2.1.2.3 Dimensions of privacy

Apart from the distinction between access and control theories privacy also has several dimensions. Clarke (2006) proposed a very widely used typology with four dimensions of privacy. Based on his work Finn et al. (2013) and Koops et al. (2017) have recently developed a more sophisticated typology, which also takes into account the current state of technical development. Finn et al. (2013) have expanded Clarke's four dimensions to seven different dimensions of privacy (see also Fig. 3):

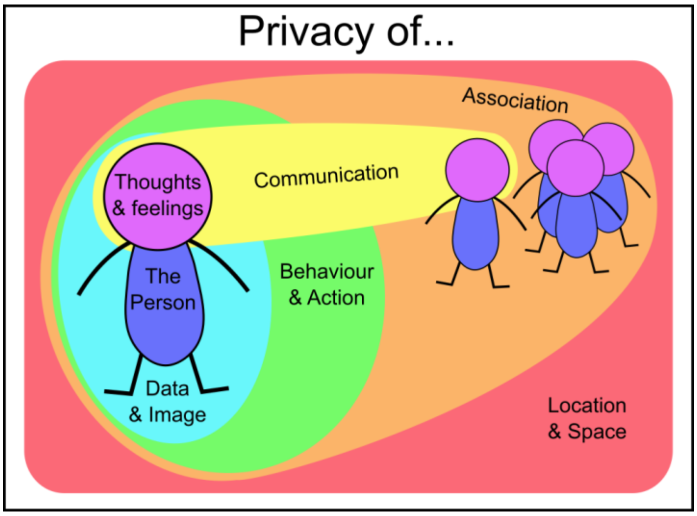


Figure 3: Seven dimensions of privacy (Source: http://www.otom.info/seven-types-of-privacy)

- *Privacy of the person* encompasses the right to keep body functions and body characteristics private. It includes the provision of protections against torture, medical treatment, the "compulsory provision of samples of body fluids and body tissue" (Clarke 2006) and imperatives to submit to biometric measurement. Mordini notes that the human body has a strong symbolic dimension as the result of the integration of the physical body and the mind and is "unavoidably invested with cultural values" (Mordini 2011). Privacy of the person is thought to be conducive to individual feelings of freedom and supports a healthy, well-adjusted democratic society.

- *Privacy of behaviour and action* includes a protection against the disclosure of sensitive personal matters such as sexual preferences and habits, political activities and religious practices. However, the notion of privacy of personal behaviour concerns activities that happen in public private space. Clarke made a distinction between casual observation of behaviour by a few nearby people in a public space with the systematic recording and storage of information about those activities (Clarke 2006). According to Nissenbaum, an ability to behave in public, semi-public or one's private space without having one's actions monitored or controlled by others contributes to "the development and exercise of autonomy and freedom in thought and action" (Nissenbaum 2009). It can be discussed if all kinds of inferred information, the so-called "behavioural surplus" (Zuboff 2019, Ch. 3) is part of this dimension as well.
- *Privacy of communication* aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages. This right is recognised by many governments through requirements that wiretapping or other communication interception must be overseen by a judicial or other authority. This aspect of privacy benefits individuals and society because it enables and encourages a free discussion of a wide range of views and options, and enables growth in the communications sector.
- *Privacy of data (including sound and images)* refers to classical data protection (data privacy) issues, but also includes capture of images and speech/sound, since these are considered a type of personal data by the European Union as part of General Data Protection Regulation (GDPR) as well as other sources. This dimension includes protecting an individual's data from being automatically available or accessible to other individuals and organisations and that people can "exercise a substantial degree of control over that data and its use" (Clarke 2006). Such control over personal data builds self-confidence and enables individuals to feel empowered. This aspect of privacy has social value in that it addresses the balance of power between the state and the person and is reflected in data protection laws and regulations in many countries.
- *Privacy of thought and feelings* is a new dimension that became necessary since new and emerging technologies also carry the potential to impact on individuals' privacy of thoughts and feelings (Zuboff 2019, Ch. 9; Hallinan et al. 2014). People have a right not to share their thoughts or feelings or to have those thoughts or feeling revealed. Privacy of thought and feelings can be distinguished from privacy of the person, in the same way that the mind can be distinguished from the body. Goold (2009) argues that the creative freedom to think and feel what one likes without being concerned about the repercussions benefits society because it relates to the balance of power between the state and the individual.
- *Privacy of location and space* refers to the assumption that individuals have the right to move in public or semi-public space without being identified, tracked or monitored. The right came under pressure with the on-going diffusion of (auto) identification and satellite location technology. This dimension of privacy also includes a right to solitude and a right to privacy in spaces such as the home, the car or the office. Such conception has social value in that individuals experience a sense of living with freedom and encourages dissent and freedom of assembly, both of which are essential to a healthy democracy.
- *Privacy of association (including group privacy)*, finally, is concerned with people's right to associate with whomever they wish, without being monitored. This has long been recognised as desirable (necessary) for a democratic society as it fosters freedom of speech, including political speech, freedom of worship and other forms of association. Society benefits from this aspect of privacy in that a wide variety of interest groups will be fostered, which may help to ensure that marginalised voices, some of whom will press for more political or economic change, are heard.

The use of such a multi-dimensional concept of privacy is useful, since new technologies, especially in the area of (cyber)security technologies, often do not influence such dimensions at all, which for example focus on data protection. Rather, privacy of location, privacy of behaviour and privacy of thoughts and feeling are currently threatened thought the use of soft biometrics, smart video-surveillance and of kinds of AI based security applications.

Regardless of the described conceptualisations of privacy, and of their general theoretical interest, as a matter of fact privacy and personal data protection as legal concepts need to be inevitably apprehended as belonging to one particular legal system. They are indeed differently shaped by each legal system, inside which, in addition, they are never stable, but unceasingly variable. This is discussed in detail in chapter 3.

2.1.3 Fairness

Fairness is the third value cluster and is related to treating equally, right or reasonable and not in contradiction to accepted societal standards (equity, equality). Fairness is also related to justice as one can expect to be judged without bias or discrimination. Finally accessibility is a part of fairness as it it means providing equal opportunities based on individual needs and capabilities (van den Poel 2019).

Fairness is also important in the context of cybersecurity since cyberthreats as well as countermeasures have different effects on different actor groups. That raises questions of fairness. Fairness is often expressed as questions of justice, equal treatment or non-discrimination. Furthermore, there is an issue of social and political legitimacy when cybersecurity measures treat certain actors differently from others, for example when certain values are impaired or fundamental rights infringed.

The first aspect to consider is the damage or loss caused by cybersecurity breaches. This is often a direct financial loss caused by broken systems, production downtimes or possible ransom payments. But maybe even a larger part of the damage is less tangible and can only be quantified indirectly or not at all. Such indirect effects include, for example, loss of reputation when it becomes known that organisations have problems with their cybersecurity. This is also the reason why so few companies publicly report security breaches (Carl 2017). Finally, possible infringements on fundamental rights, such as a loss of privacy, are serious but not measurable and therefore often considered less important than financially measurable loss. It could be regarded as unfair if the assessment of the risk was based primarily on financial considerations, because part of the risk is externalised to customers and citizens.

The second aspect concerns the responsibility and the costs for necessary countermeasures. In most cases, companies and government agencies will be responsible for implementing cybersecurity measures. This raises the question of who to protect against which cybersecurity risks. This will depend to a large extent on how the potential damages and harms are assessed. Is the infringement of a citizen right as important as a financial loss of a company? Does the state have an obligation to protect its citizens or is the responsible citizen have an obligation to protect himself? This is further complicated by the question what level of uncertainty or risk is acceptable. Those who bear the actual risk may here have a different assessment than those who have to pay for the countermeasures. Again, it could be considered unfair if only organizations or the state had the power to make these decisions.

Finally, possible side effects are a third important aspect. Many cybersecurity measures come at the expense of other values, and in most cases the individuals affected are not the ones who make the decision about these measures. In addition, these are usually social groups that are particularly vulnerable anyway. For instance, many data based profiling methods reproduce the biases that are inherent in the data sets used (Friedman et al. 1996) and thus lead to unfair discrimination, often based on the basis of race, gender, age etc. (O'Neil 2016). This problem requires a social negotiation process to reconcile objective costs and benefits but also the subjective assessment of the different stakeholder groups. In addition, it is clear that large-scale data collection for cybersecurity is problematic for reasons of fairness.

Fairness also includes accessibility, which means that everyone should have the opportunity to enjoy a guaranteed minimum level of cybersecurity within his or her means and abilities. This raises a number of fairness questions: The first one is again the question who decides what the minimal level of cybersecurity should be that operators have to offer. And, as in the case of privacy, whether it is fair that the level of protection finally depends on the financial capabilities of the individual. Therefore, there are demands to treat cybersecurity as a public good (Taddeo 2019).

Finally, there is a relationship between cybersecurity and democracy. Here we understand "democracy" as a part of fairness, because cybersecurity measures have such intrusive and distributional effects that they would require democratic legitimation rather than being decided by the competent authorities only.[22]

Cyber-attacks, which either aim to sabotage the functioning of a democratic community or to take direct influence on democratic processes, ultimately weaken citizens' confidence in democracy. An example of the first aspect were the cyber-attacks on Estonian organisations such as parliament, banks, ministries and media in 2007, which took place at the same time as protests by the Russian-speaking minority in Estonia. The second aspect can be seen, for example, in the many attempts in recent years to influence public opinion with the help of disinformation and propaganda in the so-called social media. So far, this has culminated in the Cambridge Analytica/Facebook case to influence the U.S. presidential elections in 2016 (Vrabel 2018; Susser et al. 2019).

2.1.4 Accountability

The notion of accountability is closely related to responsibility but has different meanings in different disciplines. According to Hunt (2016, p. 44), accountability "is the readiness or preparedness to give an explanation or justification to relevant others (stakeholders) for one's judgments, intentions, acts and omissions when appropriately called upon to do so. It is [also] a readiness to have one's actions judged by others and, where appropriate, accept responsibility for errors, misjudgements and negligence and recognition for competence, conscientiousness, excellence and wisdom. It is a preparedness to change in the light of improved understanding gained from others."[23] In the context of cyber security, this includes the ability of the controller to demonstrate that his activities and measures are compliant with the law. In the GDPR, for instance, the basic assumption here is that controller can be trusted by default, but that they must always be able to prove that they deserve this trust.

At the heart of the concept is therefore the interest in finding out why certain actions have been taken and, if necessary, punishing the actor in case of misconduct. In the case of cybersecurity, it is clear that we want to hold perpetrator accountable for their doings, i.e. victims have an interest to attribute the attach to an adversary. More important, however, are the risks originating from the power imbalance between big corporate and state actors on the one side and citizens and SMEs on the other. In general, companies and governments are at least accountable to customers and citizens for the cybersecurity measures they have taken (or the lack thereof).

The simplest rule is that an actor can be held accountable if (1) the actor is functionally and/or morally responsible for an action, (2) some harm was caused by that action, and (3) the responsible actor had no legitimate justification for the act. Ideally, the assumption would then be to hold the actor responsible for the action can also accountable for the results of that action. He would then be obliged to correct his wrongdoing and/or to pay the damage.

But even if there is not concrete harm, there is a duty of accountability due to the imbalance of power. The fact that people interact with organisations that can become existentially dangerous to them and to which they (must) nevertheless surrender is part of everyday knowledge – this includes on the one hand public authorities and on the other hand companies with significant market power. Under the conditions of modern, functionally differentiated societies it is therefore necessary to have safeguards in the form of general accountability (as communicated responsibility) for all important decision and actions taken in cybersecurity. This kind of accountability must include a high degree

[22] For the same reason they could also be dealt with in terms of accountability in section 2.1.4.

[23] This definition shows why van de Poel (2019) considers notions such as transparency, openness and explainability as part of "accountability".

of transparency about which risks are considered relevant and why, what precautionary measures have been taken and how to deal with any damage that nevertheless occurs.

This includes a justification why it is proportionate that specific actors/societal groups have to accept negative side effects of cybersecurity measures. These side effects may include financial costs for individual protection measures, but also an acceptable limitation of certain fundamental rights. In general, accountability here means the traceability of decisions and the documentation of the motives, assumptions and arguments behind them.

2.2 Interaction between central values

Though values themselves cannot be considered directly action guiding they provide a reason for action. For example, if cybersecurity is a value, we have reason to increase it through technical and institutional measures. If privacy is also a value, there is a reason to respect the privacy of computer users in devising such cybersecurity measures. However, it may happen that a security measure makes it necessary to interfere with privacy or that a certain security measure cannot be implemented as planned for reasons of privacy protection. This shows that different values, although all desirable, can lead to conflicts that have to be resolved with all interests in mind. Or more generally: When values are varieties of goodness, the aim of an action is to contribute to them as much as possible. However, if an action leads to a situation that contributes to one value while diminishing another, we call this a conflict of values.

In cybersecurity, such conflicts are not unusual, and the aforementioned conflict between security and privacy is certainly the best-known case. For didactic reasons such conflicts are often formulated as irreconcilable opposites: for instance, confidentiality conflicts with transparency. If data is completely confidential, no third party has access; this is the opposite of transparency. Conversely, confidentiality is not possible if the data is to be fully transparent.

In real cases, such fundamental conflicts are usually not the issue. If a value such as privacy requires confidentiality, while transparency requires the disclosure of data, then privacy transparency conflict. In a specific context, however, a solution must be found in which both values are adequately taken into account. It is also important how a value is conceptualised: obviously the concept of "privacy as confidentiality" (access theory) leads to conclusions regarding transparency than the concept of "privacy as control" where transparency is not a fundamental problem as long as the individual can adequately control it.

However, the discussion about value conflicts may distract from the fact that many values even support each other.

When decisions in the design and implementation of cybersecurity systems are made the following must be ensured (van Lieshout et al. 2015; van de Poel et al. 2011):

- All relevant conflicts are identified, from the perspective of all affected stakeholders. It should be clear that there is no super-value overriding all others (such an opinion is sometimes voiced by security politics).
- Alternative solutions are being considered. These can be technological, but also organisational solutions. Even a different framing of the problem may be useful (Valkenburg2015).

Figure 4 gives a schematic overview of the possible conflicts between the values described in the previous section. The grey rectangles represent values within the blue value clusters (here accountability is not included; Christen et al. (2017) explain this by saying that accountability is rather a procedural value). The arrows indicate positive and/or negative effects between the values. The diagram also shows instrumental relationships: cybersecurity is a means to prevent information harm and physical harm, i.e. to increase security. It also shows that cybersecurity can make use of surveillance practices, that can have a negative impact on values such as privacy, fairness and security. After all, the diagram shows that cybersecurity always requires effort, in the form of personal efforts and economic costs.

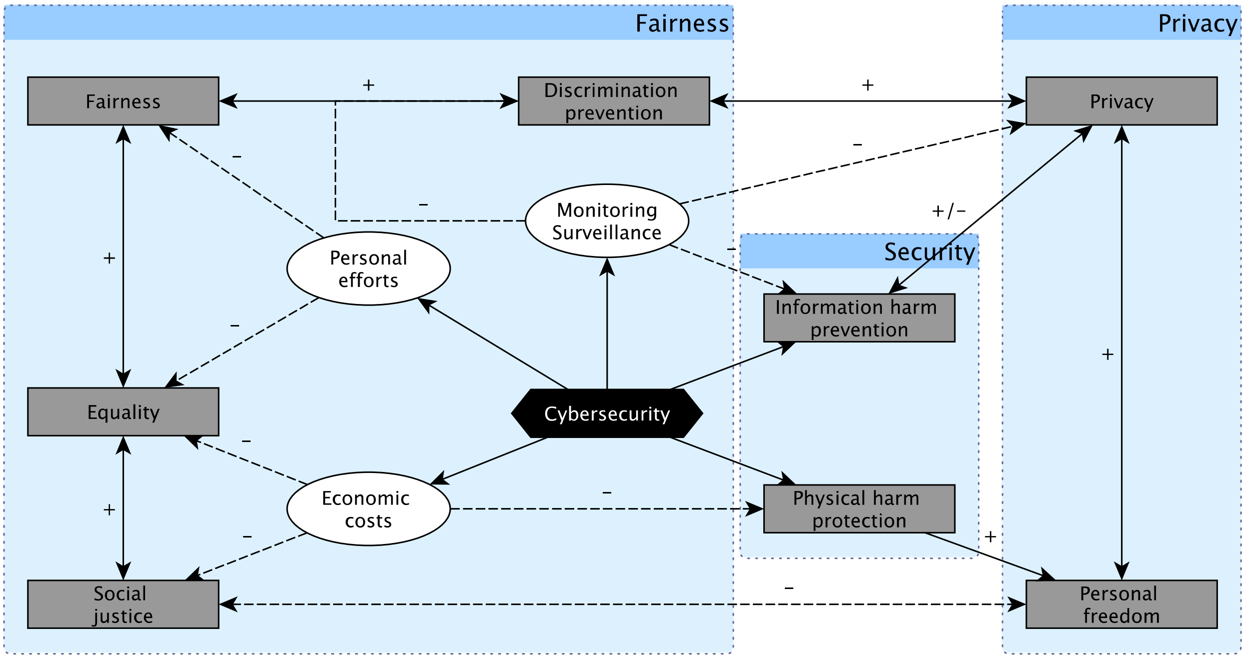


Figure 4: Interaction of values in cybersecurity according to Christen et al. (2017)

2.2.1 *Privacy vs. Security*

The relationship between privacy and security has often been seen as a trade-off, whereby any increase in security would inevitably curb the privacy enjoyed by the citizenry. Such a trade-off model has, however, been criticised, because it approaches privacy and security in abstract terms, and because it reduces privacy to one specific attitude, which considers technologies as useful in terms of security but potentially harmful in terms of privacy (Valkenburg 2015; van Lieshout et al. 2014). In the public discourse and sometimes even in the academic discussion the idea is expressed that security is a value that is inherently more important than other values, such as privacy (e.g. Bewarder et al. 2013; Himma 2016). Usually the argument says that without security a worthwhile life is not possible, in other words that security is a prerequisite for other values such as autonomy, freedom, privacy etc.

In reality the relationship between privacy and security is more complex. If values are all considered as desirable then human do not necessarily want to give up privacy in return to more security. Research has clearly shown that the attitudes towards both values are independent from one another and that citizens want to enjoy both privacy and security (Friedewald et al. 2015a; van der Broek et al. 2017).

There are a number of very different ways in which security and privacy interact with each other (Domingo-Ferrer et al. 2017):

- More security can be achieved at the expense of a loss of privacy. This is the case, for example, if network traffic is extensively monitored to identify security breaches.
- More security may contribute to more privacy. Security measures that help prevent or identify data loss or leakage contribute to the confidentiality of personal data.
- More privacy may require more security. Measures to protect personal data against unauthorised access from inside and outside an organisation contribute to the privacy.

- More privacy can be achieved at the cost of security. This is the case if user activity, including that of external attackers, remains completely anonymous and consequently attackers cannot be identified.
- More privacy can contribute to more security. If information about system details and users is confidential, external attackers cannot exploit them.

But, how then, can a conflict between security and privacy be minimized? It seems that fundamental security-privacy-conflicts only arise out of two extreme situations: (1) When too much (or even all possible) data is collected, regardless of the actual benefit of this data. In this case security definitely comes at the cost of privacy and (2) when too little (or even no) data is collected. Then privacy is achieved at the cost of security. As these situations are not very frequent privacy-security-conflicts can usually be mitigated

Therefore, the context, user constellation and system design have to be carefully analysed: (1) what data is collected and for what purpose? (2) Where and how long is the data stored? (3) Who has access to data? This shows that for a responsible handling of potential conflicts it is necessary to take extensive technical and organisational measures to ensure that the individual can exercise the most effective control possible.

2.2.2 Privacy vs. Fairness

The interaction between privacy and fairness is usually seen as mutually reinforcing. Privacy limits the amount and type of data collected. Sensitive data, such as data about ethnicity, health, sexual orientation, political beliefs etc. that could be used for unfair treatment or discrimination are particularly protected by data protection laws. A further argument is that public figures, such as politicians, who have a special accountability towards the public, also need strong privacy protection in order to be able to act independently without running the risk of being influenced by personal circumstances. In the same way democracy (as an element of fairness) is supportive to civil liberties such as privacy (Cohen 2013; Lever 2015).

There are, however, also possible conflicts between fairness and privacy. Van de Poel (2019) mentions for instance the practices to disclose private information such as income information for reasons of fair taxation.

2.2.3 Privacy vs. Accountability

As mentioned in the previous section, there is an inherent conflict between privacy and accountability because accountability requires transparency to make clear how and why someone is acting in a certain way and taking responsibility for this. The information that has to be disclosed can be privacy sensitive.

This argument is sometimes summarised under the popular slogan that "privacy is protecting perpetrators". This argument usually refers to criminals, who chose not to reveal their identity to evade from punishment for cybercrimes and cyber-attacks). The argument applies in a similar way, however, also to such persons that (mis)use privacy protection to evade their public accountability, as demonstrated by US president Trump's refusal to disclose his tax returns declaring them as private matter (Hagendorff 2018; Halstuk 2003).

Privacy (and also data protection) is not an absolute right. This means that the control over one's data can not be absolute either and there should be limits to what degree an individual can decide not to share data with others -- in particular when public interests are involved.

Finding the right balance between privacy and accountability will strongly depend from the context. It makes a difference whether a law enforcement agency wants to identify the source of hate messages on the net or whether someone demands the disclosure of an investigative journalist's sources.

2.2.4 Security vs. Accountability

Van de Poel (2019) and others argue that cybersecurity are supportive to the value of accountability. Since a lack of cybersecurity can lead to people suffering harm, the system operator must take accountability for his actions. On the other hand, a too detailed disclosure of security measures can also be exploited for malicious attacks, in such a case more accountability leads to less security. Such reasoning also comes into play when authorities try to keep undiscovered technical vulnerabilities in a system secret and exploit them as back doors for their own monitoring purposes. It is then regularly pointed out that such a lack of accountability leads to a weakening of security (see e.g. Schneier on Security[24]).

As in the case before, finding the right balance between both values requires the development of mainly organisational measures or rules that reflect which security relevant information needs to be made public for accountability reasons. Another way to resolve the tension is to disclose security information only to a publicly legitimised and accountable but otherwise closed supervisory body.

2.2.5 Fairness vs. Security

Security – especially collective security – has distributive effects. Many (cyber)security measures have an infrastructural effect, i.e. they increase the general security level for everyone. This means that for some persons they lead to an improvement in their personal security and other values, while others experience a reduction of personal security and other values. And often the improvement or deterioration of security is not at all objective, but only perceived individually. This is also the reason for a clear discrepancy in security perceptions: While many citizens feel that their personal security is high, they often feel that society as a whole is becoming less secure (Friedewald et al. 2015b). These distributive effects lead to possible tensions with (real or perceived) fairness.

This is most obvious in the case of national security. There is a great distance to citizen's normal environment, their experiences and perceptions because the objectives and means of national security are not identical to those of personal security. Controversial national security measures such as weakening crypto systems though backdoor or collecting zero-day vulnerabilities can largely put civil rights to risk, as Edward Snowden's revelations have shown some years ago (Greenwald 2014). This is particularly problematic, as such measures are usually carried out secretly and with little (perceived) legitimacy and accountability.

As our society is exposed to more and more threats from cybercrime and cyberwarfare, there is a tendency to see the level of (cyber)security as decisive factor when countermeasures are implemented. At the same time, impacts on other values are neglected. It has been argued that an overemphasis on national security can diminish the overall level of societal security.

There's also the argument that fairness means, that security gains should not be made on cost of those who are especially vulnerable and do not have the knowledge and/or resources for proper cybersecurity measures. This requires a balance between those who have the power and means to make decisions about cybersecurity (usually governments and technology companies) and those who are only affected by those decisions (Matzner et al. 2016). In this respect equality (treating everyone the same) is not enough; fairness should mean equity, i.e. giving everyone what they need according to their specific needs and abilities to protect their individual values.

2.3 Making ethical decisions

It's good to know what values to consider in cybersecurity and what value conflicts exist. But what methods can be used in concrete cases to comply with ethical requirements? There are a number of long-established concepts that could serve as a guide. In the 21st century, however, such

[24] https://www.schneier.com

established principles may need new and explicit adaptation to our emerging global technomoral environment. While the core meaning of moral principles may be fixed over time and over generations of people, the concrete meaning may be determined by the distinctive shape of a specific moral context. Especially in the domains of cybersecurity (big data, artificial intelligence), the context is one of increasingly rapid, transformative, global, unpredictable and interdependent techno-social change (Vallor 2016, p. 119). As techno-social conditions changes over time, ethical principles may have to evolve with them.

In the realm of normative ethics, three main theories are generally distinguished: utilitarianism, deontology (or Kantianism), and virtue ethics (van den Hoven 2010; Vallor 2016; Loi et al. 2019). All these theories address the same questions: What should we do and how should we act? What are the principles underpinning our actions? Or in short, what is ethical? This may translate in more practical questions such as: do we have a moral duty to tell the truth? And if so, why? Although these theories might address by and large the same question, the way in which they answer it, differs.

In deontology, morality is based on the universal law of rationality, also referred to as the categorical imperative (Kant 1998). The most important moral criterion for the categorical imperative is its universality. Why should I not lie? Because if everyone was lying, there would be no way to distinguish true from false. It would make it impossible to make rational decisions, and this would ultimately reduce human dignity. This is unattainable and hence not in accordance with the law of rationality. Universal rational consistency is the key to the deontological approach. Thus, the deontological theories are based on the moral evaluation of the action itself, rather than the result of such action.

For utilitarianism and consequentialism, morality is about maximizing the good like happiness, wealth or any other benefit and minimizing anything that diminishes the good. For utilitarians, morally just actions are those, which promote the greatest happiness of the majority. Therefore, lying may be a right action if it contributes to the happiness of most people.

Both utilitarianism and deontology are characterized by rather fixed rules and principles and both approach ethics as impartial. In utilitarian theory, there is no difference between my own happiness and that of someone else. Morality is about maximizing happiness in general and not my happiness in particular. For deontology, empirical considerations (such as introspection, psychology, biology, etc.) should not play a role in deciding what is a ethically good. What is ethically good cannot be based on a non-ethical good.

Both theories have been criticised. Utilitarianism has been criticized because it decouples the moral value of actions from the moral value of persons and thus sometimes legitimizes the well-being of a minority that is sacrificed for greater overall happiness. The deontological approach has been criticised because it values rational consistency more than the value of human relations (for instance Rössler 2005; Vallor, 2016).

Finally, modern virtue ethics can be seen as a reaction to both deontology and utilitarianism. Unlike these normative theories, virtue ethics has no supreme principle of morality. An action is considered ethically correct if it can be identified as an action that a virtuous person would undertake (Vallor 2016). It is assumed that virtuous action leads to human prosperity. But what this flourishing entails depends on the situation and can change over time. In virtue ethics it is not enough to apply only moral principles, as they are central in deontological or utilitarian ethics, to decide how to act. What a particular virtue consists of depends on the context and on the person. In virtue ethics, therefore, both rationality and more contextual and relational considerations must be taken into account.

It is assumed that acting virtuously will lead to human flourishing. But what this flourishing entails depends on the situation and can change over time. In virtue ethics, it is therefore not enough to merely apply moral principles in order to decide how to act. What a particular virtue consists of depends on the context and on that person. In virtue ethics, both rationality as well as more contextual and relational considerations must therefore be taken into account.

Since it is impossible to determine the right action in advance - that is, without taking into account the specific context - virtue ethics emphasizes the importance of practice. People should have the opportunity to explore and develop their virtues. They should learn to distinguish what are the important moral issues in a given situation and how to deal with them creatively. For example, virtue ethics will tell that lying is wrong. But not because it is against the categorical imperative and thus always wrong, but because dishonesty is an obstacle to being a virtuous person. This does not mean, however, that one should always tell the truth. A truly virtuous person knows when and with whom he can share what kind of information.

It can be argued that virtue ethics is less systematic and lacks clear criteria on which to base ones actions. However, the more flexible structure of virtue ethics seems to be better suited to the great uncertainties in a rapidly changing techno-social world. It does not conceive humans as a purely rational actors, but also pays attention to emotional disposition, relationships and the social context in which they acts. Since virtue ethics places practical wisdom above fixed rules, it is "ideally suited for adaptation to the open-ended and varied encounters with particular technologies that will shape the human condition in this and coming centuries" (Vallor 2016, p. 33). Furthermore, due of its focus on practical wisdom, a virtue-ethics approach is well suited to incorporate stakeholder insights gained in workshops and other related events into the analysis. The theory of virtue as a model has been adopted in various fields such as bioethics, media ethics and business ethics (Vallor 2016; van der Sloot 2017).

In the light of these considerations, we choose virtue ethics, rather than deontology or utilitarianism, as the main approach to deal with ethical issues. By choosing the approach of virtue ethics, we need to think about (1) what does human flourishing mean in the context of cybersecurity, (2) what are the necessary conditions to ensure this flourishing and (3) what do people need to put these virtues into practice?

The latter is closely linked to the cybersecurity technologies that are central to the SPARTA project. What are the ethical requirements for designing these technologies to ensure that citizens can develop and practise their virtues? In other words, in what ways can cybersecurity technologies facilitate people to become virtuous persons?

Chapter 3 Legal issues

As the objective of this deliverable is to identify the relevant ethical, legal and societal aspects in the context of large-scale cybersecurity research and innovation, this chapter is dedicated to the legal analysis. We focus in particular on safeguarding fundamental rights in cybersecurity research and innovation. This choice is explained by the fact that security must serve the fundamental rights recognized by the European Union.

In view of the definition of cybersecurity and its link with the preservation of confidentiality and integrity of information, we will focus in particular on the protection of personal data and the right to freedom of expression.

3.1 Key definitions

The following list includes the main definitions from the General Data Protection Regulation that are used in the document.

- **Consent:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her[25]
- **Data controller:** the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data[26].
- **Data processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller[27].
- **Identifiable natural person**: who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[28].
- **Personal data:** any information relating to an identified or identifiable natural person[29].
- **Personal data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[30]
- **Processing of personal data:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction[31].
- **Profiling:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work,

[25] Article 4.11 of the GDPR.
[26] Article 4.7 of the GDPR.
[27] Article 4.8 of the GDPR.
[28] Article 4.1 of the GDPR.
[29] Article 4.1 of the GDPR.
[30] Article 4.12 of the GDPR.
[31] Article 4.2 of the GDPR.

economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[32]

- **Pseudonymisation:** 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[33].
  It is important to keep in mind that pseudonymisation differs from **anonymisation**. If this last notion is not defined in the General Data Protection Regulation, the Directive 2019/1024 on open data and the re-use of public sector information[34] states that anonymisation refers to 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 subject is not or no longer identifiable[35]. The European Commission adds that "*Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible*"[36].

3.2 European fundamental rights framework

Several European instruments recognise the existence of different fundamental rights. These are mainly:

- Treaty on European Union;
- European Convention on Human Rights;
- European Charter of Human Rights;
- General Data Protection Regulation.

At the international level, we can highlight the International Covenant on Civil and Political Rights, the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data[37] (also known as «Convention 108+) and the Convention on the Rights of the Child.

All these instruments enshrine fundamental rights, recognized for all citizens. In particular, the main fundamental rights relevant in the context of cybersecurity are:

- The right to privacy;
- The right to the protection of personal data;
- The non-discrimination right ;
- The right to life ;
- The right to human dignity;
- The right to integrity;

[32] Article 4.4 of the GDPR.
[33] Article 4.5 of the GDPR.
[34] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, *O.J.*, L 172, 26.06.2019 (hereafter "Directive 2019/1024").
[35] Article 2.1 of the Directive 2019/1024. Furthermore, according to the former Belgian Commission de protection de la vie privée (now called Data Protection Authority), anonymization is a processing that starts with identifiable personal data and results in data that are no longer identifiable (free translation).
[36] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
[37] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg the 28 January 1981, ETS No.108 (Convention 108+, hereafter). This convention is open as other countries than the members of the CoE can join it.

- The right to freedom of expression and information;
- The right to freedom.

3.3 Fundamental rights relevant in the context of cybersecurity

As a preliminary remark, we highlight the article 2 of the Treaty on European Union which provides that "*The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail*".

Let us take up various challenges that currently arise in a society where we are increasingly confronted with technologies and the combined use of data (which may or may not be of a personal nature) and algorithms which impact the values of the European Union:

- Massive collection of personal data;
- Loss of control;
- Profiling and blacklisting;
- Malicious acts;
- Data conservation;
- Data breaches;
- Inaccuracy of the personal data;
- Surveillance.
-

3.3.1 The right to privacy

3.3.1.1 Legal basis

The right to respect for private and family life is enshrined in Article 8 of the ECHR.

> **Art. 8- Right to respect for private and family life**
>
> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

3.3.1.2 Evolution of the notion of "privacy"

In its traditional acceptance, privacy is considered as this aspect of life that is carried out in a hidden way. It is therefore a life not necessarily secret but reserved for intimates.[38]

[38] C. DE TERWANGNE, « Internet et la protection de la vie privée et des données à caractère personnel », in *L'Europe des droits de l'homme à l'heure d'Internet*, Q. VAN ENIS and C. DE TERWANGNE (dir.), Brussels, Larcier, 2019, p. 329.

As stated by the Resolution 428 (1970) from the Parliamentary Assembly of the Council of Europe: *“The right to privacy consists essentially in the right to live one's own life with a minimum of interference. It concerns private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially. Those who, by their own actions, have encouraged indiscreet revelations about which they complain later on, cannot avail themselves of the right to privacy”*[39]*.*

In this first sense, the concept of privacy guarantees the loneliness of the individual. This expression thus aims at the possibility of establishing human relations in a free manner and without any external interference. Therefore, it is the idea of the quiet zone, the space where we are free to act as we wish, where we are protected from interference.[40].

Secondly, the European Court of Human Rights, in the case *Niemitz v. Germany*, adds a fundamental element for the notion of privacy. According to the Court: “it *would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings*”[41]. In the case Peck v. United Kingdom, the Court states again that *"Private life is a broad term not susceptible to exhaustive definition (…) it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of “private life”"*[42].

Thirdly, the European Court of Human Rights[43] adds that: “*private life”, which is a broad term encompassing, inter alia, aspects of an individual’s physical and social identity including the right to personal autonomy, personal development and to establish and develop relationships with other human beings and the outside world*”[44]. Privacy is also the right to autonomy with regard to the information we decide to disclose about ourselves, the right of the individual to know what is known about him and to know the data concerning him that is held[45].

3.3.1.3 Privacy and protection of personal data

In its *z. v. Finland* judgment[46], the European Court of Human Rights states that: “*the protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention*”[47].

[39] Resolution 428 (1970), Declaration on mass communication media and Human Rights, available at: http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNTg0MiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE1ODQy

[40] C. DE TERWANGNE, « Le droit à la vie privée : quel sens aujourd’hui ? », *Quand l’invasion technologique menace nos libertés*, Bois-de-Vilers, Grappe, 2016, p. 27.

[41] ECHR, *Niemietz v. Germany*, 16 December 1992, ,° 13710/88, pt. 29.

[42] ECHR, Peck v. The United Kingdom, 28 January 2003, n°44647/98, pt. 57.

[43] ECHR, *Evan v. The United Kingdom*, 10 April 2007, n°6339/05.

[44] ECHR, *Evan v. The United Kingdom*, 10 April 2007, n°6339/05, pt. 71

[45] C. DE TERWANGNE, « Internet et la protection de la vie privée et des données à caractère personnel », in *L’Europe des droits de l’homme à l’heure d’Internet*, Q. VAN ENIS and C. DE TERWANGNE (dir.), Brussels, Larcier, 2019, p. 329.

[46] ECHR, *z. v. Finland*, 25 February 1997, n° 22009/93.

[47] ECHR, *z. v. Finland*, 25 February 1997, n° 22009/93, pt. 95.

Then, with its *Rotaru v. Romania* judgment, the European Court of Human Rights extends the concept of privacy to the protection of personal data [48]. The protection of personal data is therefore an emanation of the right to respect for private life. It is the right of everyone to control their own data, whether private, public or professional.

Later, the Court reiterates its approach: "*The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged*"[49]

Likewise, the modernised version of the Convention 108 – which is the one and only international instrument regarding the protection of personal data- states that: "*it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data*"[50].

The right to the protection of personal data has been recognised as a fundamental right in its own right in Article 16 of the TFEU and in the Charter of Fundamental Rights of the European Union. The latter explicitly distinguishes the right to respect for private life (Article 7) from the right to protection of personal data (Article 8).

- ➔ See also the Resolution 1843 (2011) of the Parliamentary Assembly of the Council of Europe: "*The Assembly recalls the fundamental human right to respect for private and family life, home and correspondence as guaranteed by Article 8 of the European Convention on Human Rights. This right includes the right to the protection of personal data as well as the obligation of states to establish appropriate safeguards under domestic law in this regard*".[51]

- ➔ See also the Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe: "*In view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to this definition*"[52].

[48] ECHR, *Rotaru v. Romania*, 4 May 2000, n° 28341/95, pt 43.

[49] ECHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*,, 27 June 2017, n° 931/13.

[50] Preamble of the Convention 108+ ; C. DE TERWANGNE, « Internet et la protection de la vie privée et des données à caractère personnel », in *L'Europe des droits de l'homme à l'heure d'Internet*, Q. VAN ENIS and C. DE TERWANGNE (dir.), Brussels, Larcier, 2019, pp. 329 and following.

[51] Resolution 1843 (2011) of the Parliamentary Assembly of the Council of Europe on the protection of privacy and personal data on the Internet and online media, available at: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML- en.asp?fileid=18039&lang=en.

[52]Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy, available at : http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16641&lang%20=en.

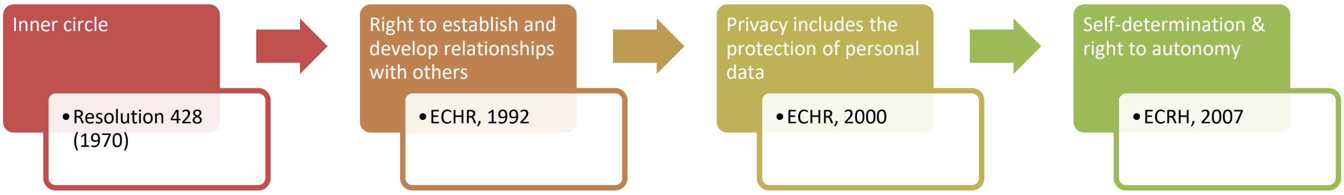

Inner circle
• Resolution 428 (1970)
Right to establish and develop relationships with others
• ECHR, 1992
Privacy includes the protection of personal data
• ECHR, 2000
Self-determination & right to autonomy
• ECRH, 2007

Figure 5: Evolution of the notion of privacy

3.3.1.4 Privacy by design

The notion of cybersecurity is intrinsically linked to the preservation of data integrity and confidentiality. These concerns are reflected in the GDPR, now making security a principle as such for the protection of personal data. Thus, article 5 provides that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accident loss, destruction or damage, using appropriate technical or organizational measures.

In the legislation, the concept of security must be integrated in the privacy by design requirement. So, in order to have a (cyber)secured product or service, the data controller has to implement technical and organizational measures to implement properly the data protection obligations.

3.3.1.4.1 Historical summary

The latest major evolution is the recognition of the principle of "privacy by design". If the previous legislation concerning the protection of personal data had prompted to that: “*Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected*”[53], the GDPR have made this in a requirement as such. For an historical overview, see the Opinion 5/2018 of the European Data Protection Supervisor (EDPS) delivered the 31th May 2018[54].

Indeed, the article 25 of the GDPR is entitled “Data protection by design and by default”:

> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement

[53] Recital 46 of the Directive (EC) 95/46 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, *O.J.*, L 281, 25.11.1995.
[54] EDPS, Preliminary Opinion on privacy by design, Opinion 5/2018, 31.05.2018, p. 3 and following.

appropriate technical and organisational measures[55], such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

According to ANN CAVOUKIAN, information and privacy Commissioner from Ontario, the 7 Foundational Principles to implement an effective privacy-by-design approach are[56]:

- *Proactive not reactive: "Privacy by Design comes before-the-fact, not after".*
- *Privacy as the default: "by ensuring the personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy"*
- *Privacy embedded into design: "privacy becomes an essential component of the core functionality being delivered"*
- *Full functionality: "Privacy by Design seeks to accommodate all legitimate interests and objectives (…). Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both".*
- *End-to-End security: "Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end".*
- *Visibility and transparency: "Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify!*".
- *Respect for User Privacy: "Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric!".*

The European Data Protection Supervisor, in its Opinion 5/2018 on Privacy by Design, delivered its conception of the various dimensions of the obligation of data protection by design. In substance, to fulfil the requirement to have an IT system which is privacy by design, all stakeholders have to be aware of the data protection principles during the whole project lifecycle. As one of the core principles

[55] According to the EDPB, "*the term measures can be understood in a broad sense as any method or means that a controller may employ in the processing. These measures must be appropriate, meaning that they must be suited to achieve the intended purpose, i.e. they must be fit to implement the data protection principles effectively by reducing the risks of infringing the rights and freedoms of data subjects. The requirement to appropriateness is thus closely related to the requirement of effectiveness*".

[56] A. CAVOUKIAN, "Privacy by Design: The 7 Foundational Principle-Implementation and Mapping of Fair Information Practices", available at: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/. These principles were reiterated at the 32nd International Conference of Data Protection and Privacy Commissioners in 2010. See their resolution on Privacy by Design: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf.

is the security of the personal data, the data controller and the data processor have to put in place a risk management approach in order to identify appropriate and effective measures. Then, the identified safeguards have to be implemented into the processing, at the beginning[57].

3.3.1.4.2 How to understand the concept of privacy by design

➔ *What are the data controller's obligations?*

The 13th November 2019, the European Data Protection Board (EDPB) adopted its Guidelines on Article 25 Data Protection by Design and by Default[58]. The EDPB insists on the fact that the safeguards for privacy of the data subjects must be implemented at the time of determining the means and the objective(s) of the processing. In addition, the data controller must, in a frequent manner, review the effectiveness of the measures put in place to ensure the respect of the GDPR's principles[59].

Therefore, the data controller has to implement:

- Technical and organisational measures;
- Which are appropriate;

According to the EDPB, "*the term measures can be understood in a broad sense as any method or means that a controller may employ in the processing. These measures must be appropriate, meaning that they must be suited to achieve the intended purpose, i.e. they must be fit to implement the data protection principles effectively by reducing the risks of infringing the rights and freedoms of data subjects. The requirement to appropriateness is thus closely related to the requirement of effectiveness*"[60].

- Integrate the necessary safeguards;
- To protect the data protection principles (article 5 and 32 of the GDPR), the data subject's rights (article 12-22 of the GDPR) and data subject's freedom (fundamental rights granted by the Charter of Fundamental Rights);
- At the time if the determination of the means for processing[61] and at the time of the processing itself.

➔ *Which elements need to be considered in order to choose the appropriate measures?*

When choosing the technical and organisational measures to be implemented, the data controller has to consider:

- The state of the art. According to the EDPB, the criteria of state of the art "*requires controllers to stay up to date on technological progress in order to secure continued effective implementation of the data protection principles*"[62].
- The cost of implementation. According to the EDPB, cost of implementation "*requires the controller to take into account the cost and resources required for the effective*

[57] EDPS, Preliminary Opinion on privacy by design, Opinion 5/2018, 31.05.2018, p. 6 and following.

[58] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

[59] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, p. 4.

[60] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, p. 4.

[61] According to the EDPB, the time of determination of the means and the objectives of the processing means: "*when the controller is in the process of determining which means must assess the appropriate measures and safeguards to effectively implement the principles and the rights of the data subjects into the processing, and take into account elements such as the 'state of the art', cost of implementation, nature, scope, context and purpose, and risks*".

According to the EDPB, "*the 'means of processing' ranges from the abstract to the concrete detailed design elements of the processing, such as the architecture, procedures, protocols, layout and appearance*".

[62] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, p. 4. For guidance on how to apply these criteria, please see p.8 of the same document.

implementation and continued maintenance of all of the data protection principles throughout the processing operation"[63].

- The nature, the scope, the context and the purpose of processing. According to the EDPB: "*the concept of **nature** can be understood as the inherent characteristics of the processing. The **scope** refers to the size and range of the processing. The **context** relates to the circumstances of the processing, which may influence the expectations of the data subject, while the **purpose** pertains to the aims of the processing*"[64].
- The risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing[65]

In parallel of the privacy by design requirements, article 25 of the GDPR imposes to the data controller to respect the privacy by default. It means that the default settings of an IT system must be designed with the data protection principles in mind. As explained by the EDPB: "*Default settings include both parameters that can be set by controllers and data subjects*"[66].

For more information, find EDPB's recommendations in Annex II.

3.3.2 The right to freedom of expression

While the products, applications and services developed within the European Union must preserve freedom of expression, one of the key challenges addressed, notably in the context of large-scale cybersecurity research, also sometimes involves considering possible legal conflicts in themselves.

Indeed, the right to privacy may conflict with the right to freedom of expression, which is also fundamental right. It is therefore a conflict between two fundamental rights since there is, in principle, no hierarchy.

3.3.2.1 Legal basis

First of all, we can identify several international instruments:

- The International Covenant on Civil and Political Rights;

> **Article 19**
>
> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;

[63] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, p. 4. For guidance on how to apply these criteria, please see p.8 of the same document.

[64] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, p. 9. See also the same reference for more information on the way to implement those criteria.

[65] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, p. 9.

[66] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, p. 4 and p. 10 and following.

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

- The Universal Declaration of Human Rights;

Article 19

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Secondly, the fundamental rights of freedom of expression is also recognized at the European level by:

- European Convention on Human Rights;

Article 10

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary

- Charter of Fundamental Rights of the European Union;

Article 11

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected.

3.3.2.2 Evolution of the notion of freedom of expression

Freedom of expression is therefore a fundamental right that enshrines the right to communicate ideas, opinions and information but also the right to receive them: it therefore has an active and a passive pole.

The European Court of Human Rights points out that freedom of expression is not limited to protecting opinions expressed in a "classical" context, i.e. in a paper press, but also in a digital environment.

Firstly, in the *Oberschlick v. Austria* judgment, the Court states that "*the Court recalls that freedom of expression, as secured in paragraph 1 of Article 10 (art. 10-1), constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual’s self-fulfilment. Subject to paragraph 2 (art. 5-2), it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb; such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society». Article 10 (art. 10) protects not only the substance of the ideas and information expressed, but also the form in which they are conveyed. This means that opinions expressed through the Internet are also under the guise of freedom of expression*”[67].

In a second evolution, in *Times Newspapers Limited v. the United Kingdom*, the Court specifies that “*Article 10 guarantees not only the right to impart information but also the right of the public to receive it. In light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10*"[68].

Finally, the Court confirms its position in the *Ashby Donald and Others v. France* judgment by recalling that article 10 of the European Convention of Human Rights is intended to apply to communication through the Internet[69].

It should be stressed that, according to the Committee of Ministers, the Internet does not change the regime applying to this freedom. Indeed, it states that "*Freedom of expression, information and communication should be respected in a digital as well as in a non-digital environment, and should not be subject to restrictions other than those provided for in Article 10 of the ECHR, simply because communication is carried in digital form*”[70].

We highlight the fact that the freedom of expression also applies on the comments and opinions even if they hurt or shock the recipient[71].

[67] ECHR, *Oberschlick v. Austria*, 23 May 1991, n° 11662/85, pt. 57.

[68] ECHR, *Times Newspapers Limited v. the United Kingdom*, 10 March 2009, n° 3002/03 and 23676/03, pt. 27.

[69] ECHR, *Ashby Donald and Others v. France*, 10.1.2013, n°36769/08, pt. 34.

[70] Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, 13 May 2005, CM(2005)56 final

[71] ECHR, *Handyside v. The United Kingdom*, 7 December 1976, n° 5493/72; ECHR, *Oberschlick v. Austria*, 23 May 1991, n° 11662/85.

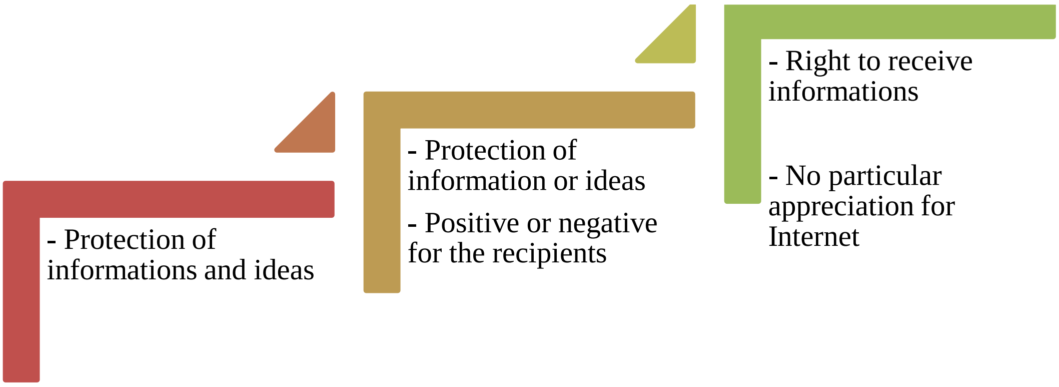

- Protection of informations and ideas
- Protection of information or ideas
- Positive or negative for the recipients
- Right to receive informations
- No particular appreciation for Internet

Figure 6: Evolution of the notion of freedom of expression

3.4 Cybersecurity and use of personal data

3.4.1 Cybersecurity and fundamental rights: the risk-based approach

As a preliminary point, it is important to recall that cybersecurity is an imperative that must be placed at the service of fundamental rights and must be considered with a view to ensuring their effectiveness, in particular the right to privacy, the right to the protection of personal data, the right to freedom of expression and the right to non-discrimination.

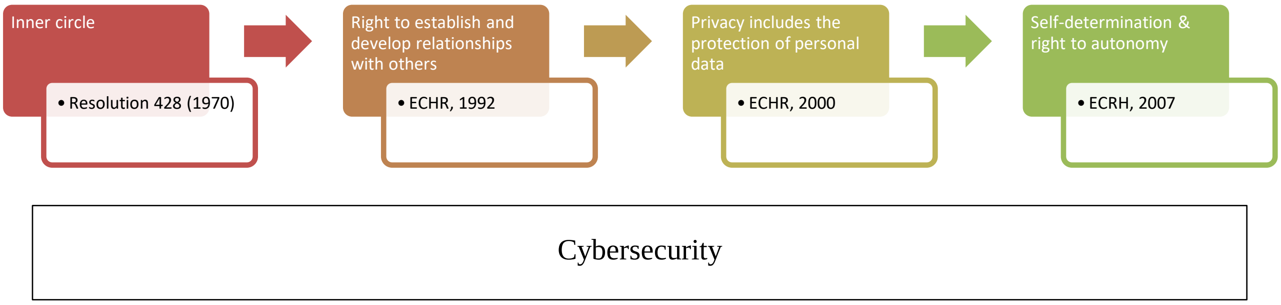

Inner circle
• Resolution 428 (1970)
Right to establish and develop relationships with others
• ECHR, 1992
Privacy includes the protection of personal data
• ECHR, 2000
Self-determination & right to autonomy
• ECRH, 2007
Cybersecurity

Figure 7: Cybersecurity and privacy components

According to the EU Cyber Security Strategy; "*cybersecurity can only be sound and effective if it based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values*"[72]. The EU insists on the fact that: "*For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace*"[73].

Moreover, when considering recital 4 of the GDPR, it can be realised that the right to protection of personal data is not an absolute right and that it must be balanced with other fundamental rights in accordance with the principle of proportionality. This Recital states that: "*The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity*".

In the same vein, the Explanatory Report of the international instrument for the protection of the personal data, the Convention 108+ insists on the fact that: "*A major objective of the Convention is to put individuals in a position to know about, to understand and to control the processing of their personal data by others. Accordingly, the preamble expressly refers to the right to personal autonomy and the right to control one's personal data, which stems in particular from the right to*

[72] European Commission, Cybersecurity Srtategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final.
[73] European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final.

privacy, as well as to the dignity of individuals. Human dignity requires that safeguards be put in place when processing personal data, in order for individuals not to be treated as mere objects”[74].

➔ We emphasize that cybersecurity is first and foremost about security. That is why one of the first steps is to identify the legal instruments that create security requirements. Let us take the concrete example of the regulation on the protection of personal data. The GDPR insists on a risk-based approach to ensure an appropriate level of security for product or service in a context where more and more information is being processed

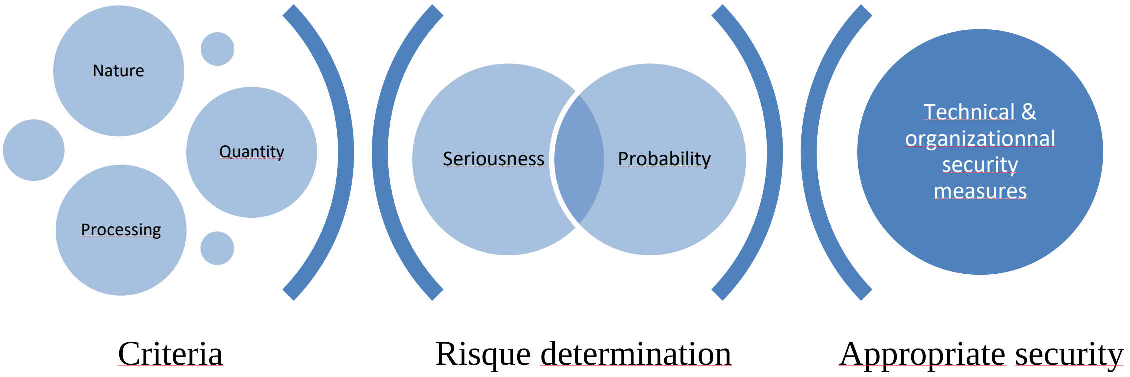


Figure 8: Appropriate security in the General Data Protection Regulation

The GDPR requires appropriate security measures and therefore takes a risk-based approach. Thus, depending on the nature, the volume of the personal data and the processing operations carried out, the controller must identify[75]:

- The risks;
- The probability that these risks will occur;
- The seriousness of the risks for people. This does not include solely risks to privacy and the protection of personal data but also to freedom of expression, freedom of thought, freedom of movement, discrimination, etc.

The Article 29 Working Party insists on the fact that the risk-based approach is not a basis for the diminution of the effectivity of the right to privacy and the protection of personal data must be understood as a scalable and proportionate manner to be compliant with the regulation[76].

➔ Second example: the NIS Directive

The NIS Directive adopts also a risk-based approach. This approach has for objective to encourage both operators of essential services and digital service providers to offer an appropriate level of security and not an absolute one.

[74] Explanatory Report of the Convention 108+, available at : https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a ; + C. DE TERWANGNE, « Internet et la protection de la vie privée et des données à caractère personnel », in *L'Europe des droits de l'homme à l'heure d'Internet*, Q. VAN ENIS and C. DE TERWANGNE (dir.), Brussels, Larcier, 2019, pp. 329 and following.
[75] Recitals 75-77 and Articles 24.1 and 32 of the GDPR.
[76] Art. 29 Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 30.05.2014, WP 218

The security of network and information systems is defined as the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems[77]. We thus find the components of the notion of cybersecurity as defined in the section above.

Recital 53 of the Directive states that: "*To avoid imposing a disproportionate financial and administrative burden on operators of essential services and digital service providers, the requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. In the case of digital service providers, those requirements should not apply to micro- and small enterprises*".

The article 14 provides for the security requirements and incident notifications to ensure the security of the network and information system of operators of essential services[78]. This articles states that: "*Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed*"[79]. Furthermore, according to article 14.4: "*In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account: (a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident*".

The same obligations exist for the security of the network and information systems of digital services providers[80]. Indeed, article 16.1 insists on the fact that: "*Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements: (a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing and testing; (e) compliance with international standards*".

Therefore, we can identify common principles for the GDPR and the NIS Directive regarding the risk management:

- The importance to adopt technical and organisational measures
- An appropriate security which depends on:
    - The risks;
    - The state of the art;

[77] Article 4.2 of the NIS Directive.
[78] Operator of essential services are public or private entity defined in the Annex II of the Directive. Each Member states has to identify concretely, in their national law, which entities are considered as operators of essential services.
[79] Article 14.1 of the NIS Directive.
[80] Digital services providers are any legal person that provides digital service (article 4.6 of the NIS Directive). Annex III of the NIS Directive establishes a list of digital services.

- Security encompasses the availability, authenticity, integrity and confidentiality of the information[81].

Finally, if the Cybersecurity Act does not impose an appropriate security as such, Recital 78 specifies that: "*the choice of the **appropriate certification** and associated security requirements by the users of European cybersecurity certificates should be based on an analysis of the risks associated with the use of the ICT products, ICT services or ICT processes. Accordingly, the assurance level should be commensurate with the level of the risk associated with the intended use of an ICT product, ICT service or ICT process*". In addition, article 8 provides for: "*ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, as established in Title III of this Regulation, by: (a) monitoring developments, on an ongoing basis, in related areas of standardisation and recommending **appropriate technical specifications** for use in the development of European cybersecurity certification schemes pursuant to point (c) of Article 54(1) where standards are not available*".

An interest correction could be made between the risk-based approach and the emergence of the "by design" concept in the EU legislative measures. Indeed, the two approaches are complementary and require developers and/or data controllers to think from the outset about the tool or service they wish to develop and to consider legal aspects in their technological developments from the outset[82]. As explained in the literature: "*The growing interest for the 'by design' approach can be seen as an alignment of what Lessig has called the West Coast and the East Coast Code. The East Coast Code (a reference to Washington DC, USA) is the Law as it has been intended so far, namely all the statutes that prescribe how to behave following the logic of 'command and control' (i.e. the establishment of standards and targets as well as sanctions in case of non-compliance). This system is as old as the institution government. The West Coast Code, on the other hand, is the code that the computer engineers 'enact', the instructions embedded in the software and hardware that make the cyberspace work. In that theoretical conceptualisation, SbD (*Security by Design*) and DPbD (*Data Protection by Design*) would represent the contact points between both Codes, allowing law to overcome technological barriers and to be more efficient*"[83].

- Security is a principle as such to ensure the lawfulness of the processing of personal data (article 5 of the GDPR). According to article 32 and article 25 of the GDPR, the obligation to adopt a risk-based approach in order to determine the appropriate technical and organisational measures to ensure the security of the personal data has to be made at the earlier state of development.

[81] We highlight that, on the contrary to the GDPR, the NIS Directive does not limit its scope to the personal data. In addition to the risks and the state of the art, the GDPR imposes that the security measures decided by the data controller consider the volume of the personal data, the nature of the personal data and the purposes.

[82] D. ORLANDO and P. DEWITTE, "The 'by design' turn in EU cybersecurity law: Emergence, challenges and ways forward", *in Security and Law*, A. VEDDER, J. SCHROERS, CH. DECUING and P. VALCKE (eds.), Cambridge, Intersentia, 2019, p. 242.

[83] D. ORLANDO and P. DEWITTE, "The 'by design' turn in EU cybersecurity law: Emergence, challenges and ways forward", *in Security and Law*, A. VEDDER, J. SCHROERS, CH. DECUING and P. VALCKE (eds.), Cambridge, Intersentia, 2019, p. 242.

- Recital 12 of the Cybersecurity Act underlines the importance to build in strong security mechanisms by design: *"Organisations, manufacturers or providers involved in the design and development of ICT products, ICT services or ICT processes should be encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised ('security-by-design'). Security should be ensured throughout the lifetime of the ICT product, ICT service or ICT process by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation*". Furthermore, article 51 of the Cybersecurity Act concerning the security objectives of European cybersecurity certification schemes specifies that: "A European cybersecurity certification scheme shall be designed to achieve, as applicable, the following security objectives: (i) that ICT products, ICT services and ICT processes are secure by default and by design"[84].

3.4.2 Cybersecurity and personal data: privacy and data protection issues

3.4.2.1 Transparency/foreseeability/Public awareness

The right to data protection requires considering, on the one hand, the imbalances of power between the data subject and the data controller, imbalances generated by the latter's data processing capacities (this issue seems to be dramatically exacerbated nowadays with the speed and opacity of the technical developments) and, on the other hand, the impact that data processing may have on the various rights and freedoms of individuals[85].

In order to counterbalance this imbalance, it is important that the controller complies with the requirements of the regulation[86]. The obligation to provide information depends on:

- Whether the information is collected directly from the data subject;
- While the information is considered as mandatory by the GDPR or optional and must be provided by the controller only when necessary to ensure a fair processing, without any surprise for the data subject.

▶ **Key question: what level of transparency?** Indeed, too much transparency could have the perverse effect of disclosing valuable information about the security of a product or service, thereby increasing the risk of security attacks.

3.4.2.2 Purpose and lawfulness principle

All personal data must be processed only for specified, explicit and legitimate purposes[87]. This is the principle of purpose limitation that will allow the data controller to determine with regards to the objectives:

[84] On this point, see also D. ORLANDO and P. DEWITTE, "The 'by design' turn in EU cybersecurity law: Emergence, challenges and ways forward", *in Security and Law*, A. VEDDER, J. SCHROERS, CH. DECUING and P. VALCKE (eds.), Cambridge, Intersentia, 2019, pp. 245-246.
[85] Recital 58 of the GDPR.
[86] See articles 11-14 of the GDPR
[87] Article 5.1, b) of the GDPR.

- The personal data he/she can collect and process;
- What he/she can and cannot do with the personal data;
- The duration of the personal data retention.

Concretely, this principle requires the data controller to determine, prior to any processing or collection of personal data, for what reasons such data are used and for what purposes.

In addition, after having defined an objective, the data controller must determine a legal basis for collecting or processing personal data. Indeed, the GDPR provides that the processing is lawful only if and to the extent that at least one of the following applies[88]:

- Consent of the data subject;
- The processing is necessary for the performance of a contract to which the data subject is party;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller.

Furthermore, the objective must be explicit and cannot be vague or imprecise[89]. For example, the purposes as “Promote safety and security” or “Provide, improve and develop services” are rejected[90].

▶ **Key questions:**

- 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?

3.4.2.3 Minimisation principle

Article 5 of the GDPR states that the personal data must be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed[91]. This principle can be declined in several obligations:

- To ensure that there is no excessive usage of personal data;
- To use the data for only the authorized purpose;
- To determine the access rules;
- To determine the adequate storage period.

[88] Article 6 of the GDPR.

[89] Recital 39 and Article 12.1 of the GDPR.

[90] C. DE TERWANGNE, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », *in Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. DE TERWANGNE et K. ROSIER (coord.), Brussels, Larcier.

[91] Article 5.1 d) of the GDPR.

- **Key questions:**
  - How much data and what data need to be gathered?
  - What data should be accessible to whom?
  - For how long should these data be stored?

3.4.2.4 Availability and security

Availability is an integral part of the data protection requirements. The notion of availability refers to the possibility of the information, the systems and the processes to be accessible and usable on demand from an authorized natural person or an entity[92]. This requirement is considered by Article 29 Working Party as the third fundamental safety criterion, with confidentiality and integrity[93].

In addition, according to ENISA, « *one of the core obligations for data controllers and processors in GDPR is that of the security of personal data. In particular, according to GDPR security equally covers confidentiality, integrity and availability*"[94].

The Article 29 Working Party includes in the notion of the availability of personal data[95] :

- The destruction of the personal data;
- The accidental or unlawful loss of personal data;
- The accidental or unlawful loss of access to the personal data. This consideration is based on a definition from the National Institute of Standards and Technology according to which the availability has to be understood as a « timely and reliable access to and use of information.[96]

The Cybersecurity Act expects that ICT products, services and processes will be assessed to verify their compliance, from the design stage, with the specified security requirements, namely the guarantee of the availability, authenticity, integrity or confidentiality of the stored data, whether or not they are personal data[97].

- **Key question**: What balance must be struck between the confidentiality requirements, the availability requirements and the right to erasure granted to the data subjects?

3.4.2.5 Accountability

According to article 5.2 of the GDPR, the data controller is responsible for compliance will all the principles explained above. In addition, he/she must be able to demonstrate the compliance.

On the matter of cybersecurity, the data controller must be able to demonstrate to the data protection authority that he/she has carried out a risk analysis and has taken appropriate technical and organisational measures to minimise the risk[98].

[92] CPVP, « note relative à la sécurité des données à caractère personnel », p. 1.

[93] Art. 29 Working Party, Opinion 03/2014 on Personal Data Breach Notification, 25.03.2014, WP 213.

[94] ENISA, "Guidelines for SMEs on the security of personal data processing", December 2016.

[95] Art. 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP 250.

[96] NIST SP800-53rev4

[97] Article 51 of the Cybersecurity Act ; F. DUMORTIER, « Chapter VI – Security and incident reporting requirements », *in* GARZANTI, O'REGAN, DE STREEL and VALCKE (eds), *Electronic communications, audiovisual services and the internet: Competition Law and Regulation*, Sweet & Maxwell, 2019 (to be published).

[98] Article 32 of the GDPR.

Regarding the cybersecurity concern, the data controller must follow different steps:

- To elaborate a risk analysis. It implies for the data controller to have a full understanding of their processing, the volume and the nature of the personal data used and the consequences for the data subjects;
- Implement the technical and organisational measures;
- To be able to demonstrate the risk analysis and the answer given to minimize those risks.

Additionally, the literature insists on the fact the data controller shall: "*ensure the consistency and relevance of the trade-offs made during the design phase throughout the entire personal data lifecycle. Therefore, DPbD (*Data Protection by Design*) is not limited to legal countermeasures nor can it be reduced to the ex-post implementation of purely technical Privacy Enhancing Technologies (PETs) into existing systems'*[99].

- ▶ **Key questions: Who will be responsible** in case of data breaches? The users? The creators of the algorithms? The one who collects the datasets? Etc

- ▶ **How can PETs** be integrated into a more global reflection on the management of personal data and the risks generated by the activities and processing of the controller?

3.4.2.6 Sharing of information/personal data

In the creation of products or services, it often happens that several stakeholders are involved. This often leads to a significant data flow.

In this respect, the GDPR recognises two qualities: being a data controller or being a data processor. The data controller is the person who is responsible for ensuring compliance with the regulations and for being able to demonstrate, in the event of control by a national protection authority, that all principles and obligations have been respected.

The data processor, on the other hand, acts in the name and on behalf of the controller and under his instructions.

It should be noted, however, that the GDPR does not, as such, assign obligations and responsibilities to producers of products, services or applications. Recital 78 reflects this approach: "*The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with*

[99] D. ORLANDO and P. DEWITTE, "The 'by design' turn in EU cybersecurity law: Emergence, challenges and ways forward", *in Security and Law*, A. VEDDER, J. SCHROERS, CH. DECUING and P. VALCKE (eds.), Cambridge, Intersentia, 2019, p. 244.

due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders".

- **Key questions: What data sharing model** between operators working in security? How to distribute the roles of the different stakeholders?

Chapter 4 Societal perspective

4.1 Public attitudes towards cybersecurity

Empirical studies have shown that public attitudes to values such as privacy and security are neither simple nor monocausal. In typical security settings (not only with Cybersecurity, but especially there) they do not depend only on the types of technologies used and the amount of data collected, but even more on the purpose communicated towards citizens, the type of organisation organising and operating a security measure and very much on the concrete context in which security technology is used (Friedewald et al. 2017; Wenger et al. 2017; Pavone et al. 2017).

For the design and introduction of security measures it is thus useful to consider some of the main socio-demographic determinants for acceptance of these measures, since poorly designed measures can consume significant resources without achieving either security or privacy while others can increase security at the expense of privacy. The most important among these determinants are:

- *Context and purpose*: Public attitude depends crucially on the security issue, as the degrees of acceptance highly differ for varying privacy intrusive or value infringing situations. It makes a difference, for instance if video surveillance is used at a football match or at a political demonstration even if the purpose is the same - the identification of possible perpetrators. I can be stated that citizens make a distinction between actions that may counter a legitimate interest of EU citizens (gathering for demonstrations as a fundamental right) and actions that are meant to safeguard the majority of EU citizens (and protect them against potential violent behaviour with no direct legitimate basis) (Pavone et al. 2015; Friedewald et al. 2015b).
- *Trust*: Empirical studies – dating back to Alan Westin's studies in the 1970s (Kumaraguru at al. 2005) – have identified "trust" as one the most important factor influencing privacy and security attitudes of citizens (for more recent studies see Lusoli et al. 2012; Zureik et al. 2010). Especially trust in institutions plays a relevant role, and trust in public institutions usually correlates positively with acceptance of security practices (Pavone et al. 2015; Friedewald2015b).

  Most demographic variables have an expectable influence on trust and public opinion towards security: left-wing oriented citizens are more critical of public actors’ activities than right-wing citizens; citizens who are more critical with respect to their privacy are more critical of public intervention while people who expressed a higher security concern show a higher level of acceptance of these practices. A higher level of education is correlated with higher resistance to security interventions (Friedewald et al. 2015b).

  In general, trust reduces the complexity people need to face. Instead of making rational judgements based on knowledge, trust is employed to select actors who are trustworthy and whose opinions can be considered accurate and reliable. People having trust in the authorities and management responsible for the technology perceive less risk than people who lack that sense of trust in those members (Earle et al. 1995).

- *Transparency*: Transparency has a positive effect on the willingness of citizens to accept security practices. This can be understood on different levels: (1) Citizens tend to accept security practices when they are convinced that a security measure is necessary, proportional and effective. (2) This is easier when a security practice is embedded in a context that citizens are familiar with and where they understand who is doing what and how. (3) As a result the security measures should not be covert but perceivable for the citizen and communicated in a responsible way by the operator. (4) Understanding and acceptance is also a question of proper knowledge and education -- though not only in one way. While education contributes to understanding technicalities and complexity of a security practices it also drives critical reflections (Pavone et al. 2015; Friedewald et al. 2015b).

- *Accountability*: The type of actor (whether from the public or private sector) which operates a security solution and collects and processes personal data is relevant: at least in Europe public sector actors receive higher levels of acceptance than private sector actors. This is related to the fact that citizens often don't see that their own interest and those of a private company are aligned: Due to the imbalance of power, companies, but also the state, are in a position to take measures to assert their own interests at the expense of the individual. Citizens do not believe that private-sector actors – other that the state – feel accountable for such behaviour (Pavone et al. 2015; Friedewald et al. 2015b).
- All these factors also involve an inherent risk for manipulation, since a security practice can be designed to create false trust among citizens to be accepted.

In the arena of cybersecurity there are at least two camps. Law enforcement and government officials often heavily weight security. Civil society organisations are often critical with respect to the necessity, appropriateness and effectiveness of many hyped technologies. In this area of tension, citizens must find a position for themselves. Depending on the influencing factors described above, essentially four different types of reactions can be expected (Conti et al. 2014):

1. Citizens may consider a measure as useless to enhance security, and at the same time invasive for their privacy. Such a situation has to be absolutely avoided.
2. Citizens may consider a measure useless to enhance security but with no risk for their privacy. In the best case such measures are regarded as fig leaves or symbolic actions.
3. Citizens may consider a measure as useful in terms of security, but privacy invasive. This is a difficult case that needs to proactively addressed.
4. Finally, citizens may consider a measure both useful to increase security and with no risk for their privacy.

Citizens’ perceptions do not (always) have to reflect the real effectiveness of a security measure and its real impact on privacy and other rights and freedoms. Considering the importance of trust for the acceptability and acceptance the responsible parties should aim to reconcile the perceived and real impacts. Potential for conflicts can be mainly found at the border between reaction types 2 and 3 when citizens fear an invasion of their privacy or perceive a technology as ineffective.

For the design and introduction of cybersecurity measures it is useful to consider the main determinants, since poorly-designed measures can consume significant resources without achieving either security or privacy while others can increase security at the expense of other values. However, since there is no natural trade-off between privacy and security, carefully designed solutions can benefit both privacy and security.

4.2 Designing systems for society readiness

The previous chapters emphasized the importance of values, culture, ethical, social and legal aspects of cybersecurity. It was particularly highlighted that these aspects are crucial factors with regard to the individual and collective perception of (cyber)security. Taking these perspectives systematically and sincerely into account when designing and implementing cybersecurity applications and measures remains challenging for governance actors, developers and service providers alike. The challenge is at least fourfold:

1. The lack of knowledge about how future users will perceive a service and/or an application in terms of its security and privacy and other dimensions;
2. the knowledge deficit about how users will actually apply a service and which unforeseen practices emerge while using a newly emerging technology;
3. the difficulty of effectively translating values, cultural and ethical considerations into the design and the functions of cybersecurity applications; and
4. the challenge of anticipating and eventually avoiding unintended consequences.

In general, these and related challenges apply for the design and development of most emerging technologies as well. In technology assessment (TA) literature these challenges are often referred to by the so-called *Collingridge dilemma*, according to which there is an information deficit about the effects of a technology in early stages of development and application, whereas it becomes increasingly difficult to change a technological trajectory once the effects become more and more available (Collingridge 1980). As a response, a number of approaches have been developed in the past to better deal with the multiple challenges of lack of knowledge about the effects of technologies for individuals and society. These include numerous variants of Technology Assessment, ELSA research, foresight, risk assessments, value sensitive design etc (see for instance Spiekermann 2016; Spindler et al. 2020). The rather recent concept of *Responsible Research and Innovation* (RRI) explicitly draws on these approaches and combines key features with the aim to better align research and innovation with societal values and expectations (Owen et al. 2012; Stilgoe et al. 2013; Schomberg 2014). RRI is now a key concern in European R&I policy and it is integrated as a cross-cutting objective in H2020 (Council decision 2013).

4.2.1 Societal readiness: Increasing reflexivity

In view of the knowledge deficits mentioned above, the central aim of the RRI framework and related tools is to support researchers and innovators to become more aware of social desirability and acceptability, thereby directing responsibilities towards the future, not the past. The broad literature on RRI can be differentiated by procedural approaches and by approaches based on a number of key elements of responsibility. The key procedural conditions usually promoted by RRI frameworks are:

- **Anticipation** is understood as 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** refers to 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. (Owen et al. 2012; Stilgoe et al. 2013; Nielsen et al. 2018).

Taken together, these four procedural conditions have the potential to support forward-looking, reflexivity-conducive approaches to R&I activities. In addition to the procedural approaches, key elements of responsibility, which are primarily promoted by the EC, are public engagement, open access, science education, gender, ethics and governance.[100]

4.2.2 Thinking Tool

Despite the development of approaches aiming to better align research and innovation (R&I) with societal perspectives, concrete methods for putting RRI ambitions - both the procedural conditions and the key elements of responsibility - into research and development practices continue to be rare. One of the promising methods in this regard is the Societal Readiness Tool developed by the EU-

[100] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation

funded NewHoRRIzon project[101]. The tool offers guidance for scientists, developers and engineers who want to increase the societal readiness of their research and development outputs. The tool's claims to be a practical tool for implementing RRI into R&I practices is based on a stage-gating approach which divides common research and development processes into discrete stages intermitted by decision gates. At each stage, the technology innovation will be assessed according to certain assessment criteria. The tool's four key stages are

1. Ideation process;
2. data collection and experimental testing;
3. data analysis, evaluation and interpretation of results; and
4. launching of R&D outputs and dissemination of results (Nielsen et al. 2018).

For each of the stages, a set of questions fostering RRI perspectives needs to be answered by the user. In stage one, for instance, the user is asked to answer "who might be excluded from the benefits of the research/technology, and how will this be addressed?". In stage three, for example, a question to be answered is "how may the data analysis and evaluation best be documented to ensure transparency and allow for replication and knowledge transfer?".

In effect, the tool supports researchers to take into account and consider perspectives that are usually not in the scope of conventional R&I processes, and can thereby increase self-reflection capacities. The “Thinking Tool” is publically available at https://www.thinkingtool.eu/.

In the next stage of the SPARTA project it is intended to make use of the “Thinking Tool” to find an inroad into assessing the societal readiness of the concepts developed by the SPARTA programs.

[101] https://newhorrizon.eu/

Chapter 5 Summary and Conclusion

The term cybersecurity is a conglomerate of different elements. In this deliverable, we highlight mainly four value clusters: security, privacy, fairness and accountability.

Each of these four concepts has various dimension, summarized in the following table.

Security	Privacy	Fairness	Accountability
International security	Person	Damage or loss caused by cybersecurity breaches	Responsibility
National security	Behaviour and action	Responsibility and cost for countermeasures	Explanation
Corporate security	Communication	Accessibility	
Social security	Thought and feelings	Transparency	
Individual security	Location and space	Context and purpose	
Integrity, confidentiality and *authenticity* of personal data	Personal data		
	Association		

After identifying what values in cybersecurity are at stake and their interaction (privacy vs. fairness, privacy vs. accountability, security vs. accountability, fairness vs. security), there are several methods that can be used in concrete cases to comply with the ethical requirements; utilitarianism, deontology and virtue ethics. In this deliverable, we insist on virtue ethics in order to avoid the supreme principle of morality. By choosing this approach, we need to consider what does human flourishing mean in the context of cybersecurity? What are the necessary conditions to ensure this flourishing? What do people need to put these virtues into practice?

Furthermore, it is necessary to add an extra layer: The General Data Protection Regulation. Data protection raises several key questions to manage personal data, e.g. what level of transparency? How much data and what data need to be gathered? What data should be accessible to whom? How long should the data be stored? Who will be responsible in case of data breaches? How can PETs be integrated in a more global reflection on the management of personal data and the risks generated by the activities and processing of the data controller?

A cross-cutting principle of this deliverable is the risk management approach. Thus, all stakeholders active in the cybersecurity sector must put in place and develop policies and tools to identify the risks related to their activities and the methods to minimise them.

Chapter 6 List of Abbreviations

Abbreviation	Translation
GDPR	General Data Protection Regulation
PETs	Privacy Enhancing Technologies
R&I	Research and innovation
R&D	Research and development
RRI	Responsible research and innovation
ENISA	European Network and Information Security Agency
TA	Technology Assessment
ELSA	Ethical, Legal, Societal Aspects
H2020	Horizon 2020 (8th Framework Programme for Research and Innovation)
EC	European Commission

Chapter 7 Bibliography

Allen, Anita L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Totowa, N.J.: Rowman & Littlefield.

Bewarder, Manuel and Thorsten Jungholt (July 16, 2013). “Friedrich erklärt Sicherheit zum ‘Supergrundrecht’”. In: *Die Welt*. URL: https://www.welt.de/politik/deutschland/article118110002/Friedrich-erklaert-Sicherheit-zum-Supergrundrecht.html.

Brooks, David J. (2009). “What is security? Definition through knowledge categorization”. In: *Security Journal* 23.3, pp. 225–239. DOI: 10.1057/sj.2008.18.

Carl, Sabine (2017). “An unacknowledged crisis: Economic and industrial espionage in Europe”. In: *Europe in Crisis: Crime, Criminal Justice, and the Way Forward*. Ed. by C.D. Spinellis et al. Athens: Ant. N. Sakkoulas, pp. 755–761.

Cavoukian, Ann, “Privacy by Design: The 7 Foundational Principle-Implementation and Mapping of Fair Information Practises“. URL: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/

Census Act (Dec. 15, 1983). Decisions of the Federal Constitutional Court (Entscheidungen des Bundesverfassungsgerichts – BVerfGE) 65, 1. URL: https://www.bundesverfassungsgericht. de / SharedDocs / Entscheidungen / EN / 1983 / 12 / rs19831215 _ 1bvr020983en . html (visited on 12/06/2010).

Christen, Markus, Bert Gordijn, and Michele Loi, eds. (2019). *The Ethics of Cybersecurity*. Vol. 21. International Library of Ethics, Law and Technology. Cham: Springer. DOI: 10.1007/978-3-030-29053-5.

Christen, Markus et al. (Dec. 2016). “Using thesauruses as a heuristics for mapping values”. In: *Cognitive Systems Research* 40, pp. 59–74. DOI: 10.1016/j.cogsys.2016.02.003.

Christen, Markus et al. (Sept. 2017). “A Review of Value-Conflicts in Cybersecurity: An assessment based on quantitative and qualitativeliterature analysis”. In: *ORBIT Journal* 1.1. DOI: 0.29297/orbit.v1i1.28.

Clarke, Roger (2006). *What’s Preivacy?* Prepared for a Workshop at the Australian Law Reform Commission on 28 July 2006. Chapman, Australia: Xamax Consultancy. URL: http://www.rogerclarke.com/DV/Intro.html (visited on 10/22/2019).

Cohen, Julie E. (2013). “What privacy Is for”. In: *Harvard law review* 128, pp. 1904–1933.

Collingridge, David (1980). *The social control of technology*. New York: St. Martin’s Press.

Conti, Gregory, Lisa Shay, and Woodrow Hartzog (2014). “Deconstructing the Relationship between Privacy and Security”. In: *IEEE Technology and Society Magazine* 33.2, pp. 28–30.

De Terwangne, Cécile (2016), “Le droit à la vie privée : quel sens aujourd’hui?“. In: *Quand l’invasion technologique menace notre libertés,* Bois-de-Vilers, Grappe.

De Terwangne, Cécile (2019), *Le règlement général sur la protection des données (RGPD/GDPR)-Analyse approfondie*, Brussels, Larcier.

Domingo-Ferrer, Josep et al. (Dec. 21, 2017). *Technological Challenges in Cybersecurity*. White Paper 4. CANVAS Project. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091942.

Earle, Timothy C. and George Cvetkovich (1995). *Social trust: Toward a cosmopolitan society*. Westport, Conn.: Praeger.

Council decision (December 20, 2013): “Council decision of 3 December 2013 establishing the specific programme implementing Horizon 2020 - the Framework Programme for Research and

Innovation (2014-2020) and repealing Decisions 2006/971/EC, 2006/972/EC, 2006/973/EC, 2006/974/EC and 2006/975/EC". In: *O.J.* L 347, pp. 965-1041. DOI:10.3000/19770677.L_2013.347.eng

Fairfield, Joshua A. T. and Christoph Engel (2015). "Privacy as a social good". In: *Duke Law Journal* 65.3, pp. 385–457.

Finn, Rachel L., David Wright, and Michael Friedewald (2013). "Seven types of privacy". In: *European Data Protection: Coming of Age*. Ed. by Serge Gutwirth et al. Dordrecht: Springer, pp. 3–32. DOI: 10.1007/978-94-007-5170-5_1.

Ford, R. Glenn and David W. Krumme (1979). "The analysis of space use patterns". In: *Journal of Theoretical Biology* 76.2, pp. 125–155.

Freud, Siegmund (1957). "Thoughts for the times on war and death [1915]". In: *Works*. Ed. by James Strachey. Vol. 14. London: Hogarth Press, pp. 275–300.

Fried, Charles (1970). *An Anatomy of Values: Problems of Personal and Social Choice*. Cambridge: Harvard University Press.

Friedewald, Michael et al. (2015a). "Privacy and Security Perceptions of European Citizens: A Test of the Trade-off Model". In: *Privacy and Identity 2014, IFIP AICT, vol. 457*. Ed. by Jan Camenisch, Simone Fischer-Hu˙bner, and Marit Hansen. Heidelberg, Berlin: Springer. Chap. 4, pp. 39–53. DOI: 10. 1007/978-3-319-18621-44.

Friedewald, Michael et al. (Oct. 2015b). *Report on the analysis of the PRISMS survey*. Deliverable 10.1. PRISMS project. URL: http://publica.fraunhofer.de/documents/N-367427.html.

Friedewald, Michael et al., eds. (2017). *Surveillance, Privacy and Security: Citizens' Perspectives*. PRIO New Security Studies. London: Routledge. DOI: 10.4324/9781315619309.

Friedman, Batya and Helen Nissenbaum (1996). "Bias in computer systems". In: *ACM Transactions on Information Systems* 14.3, pp. 330–347. DOI: 10.1145/230538.230561.

Goold, Benjamin J. (2009). "Surveillance and the Political Value of Privacy". In: *Amsterdam Law Forum* 1.4, pp. 3–6. URL: http://www.amsterdamlawforum.org/.

Greenwald, Glenn (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.

Gutwirth, Serge (2002). *Privacy and the Information Age*. Lanham, Boulder, New York, Oxford: Rowman & Littlefield.

Gutwirth, Serge et al. (Mar. 23, 2011). *Legal, social, economic and ethical conceptualisations of privacy and data protection*. Deliverable 1. PRESCIENT Project. DOI: 10.5281/zenodo.1182961.

Hagendorff, Thilo (2018). "Die Ambivalenz des Privaten". In: *Privatheit und selbstbestimmtes Leben in der digitalen Welt*. Ed. by Michael Friedewald. Wiesbaden: Springer Vieweg, pp. 13–32.

Hallinan, Dara et al. (2014). "Neurodata and Neuroprivacy: Data Protection Outdated?" In: *Surveillance Society* 12.1, pp. 55–72. ISSN: 1477-7487. DOI: 10.24908/ss.v12i1.4500.

Halstuk, Martin E. (2003). "Shielding Private Lives from Prying Eyes: The Escalating Conflict between Constitutional Privacy and the Accountability Principle of Democracy". In: *CommLaw Conspectus* 11, pp. 71–96.

Haney, Craig (2003). "Mental health issues in long term solitary and supermax confinement". In: *Crime and Delinquency* 49.1, pp. 124–156.

Himma, Kenneth E. (2016). "Why security trumps privacy". In: *Privacy, security, and accountability: ethics, law and, policy*. Ed. by Adam D. Moore. London; New York: Rowman & Littlefield, pp. 145–170.

Hunt, Geoffrey (2016). “The Principle of Complementarity: Freedom of Information, Public Accountability and Whistleblowing”. In: *Open Government in a theoretical and practical context*. Ed. by Richard A. Chapman and Michael Hunt. London and New York: Routledge, pp. 43–53.

Johnson, Deborah J. and Keth W. Miller (2003). *Computer Ethics: Analyzing Information Technology*. 4th ed. Upper Saddle River, NJ: Prentice Hall.

Kant, Immanuel (1998). *Groundwork of the Metaphysics of Morals [1785]*. Cambridge and New York: Cambridge University Press.

Kasper, Debbie V. S. (2007). “Privacy as a Social Good”. In: *Social Thought and Research* 28, pp. 165–189.

Koops, Bert-Jaap et al. (2017). “A Typology of Privacy”. In: *University of Pennsylvania Journal of International Law* 38.2, pp. 483–575.

Kumaraguru, Ponnurangam and Lorrie Faith Cranor (Dec. 2005). *Privacy Indexes: A Survey of Westin’s Studies*. ISRI Technical Report CMU-ISRI-05-138. Carnegie Mellon University. URL: http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf.

Lagazio, Monica (Sept. 2012). “The evolution of the concept of security”. In: *The Thinker* 43.9, pp. 36–43.

Lever, Annabelle (2015). “Privacy, Democracy and Freedom of Expression”. In: *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Ed. by Dorota Mokrosinska and Beate Roessler. Cambridge: Cambridge University Press, pp. 162–180. DOI: 10.1017/CBO9781107280557.010.

Loi, Michele and Markus Christen (2019). “Ethical Frameworks for Cybersecurity”. In: *The Ethics of Cybersecurity*. Ed. by Markus Christen, Bert Gordijn, and Michele Loi. Vol. 21. International Library of Ethics, Law and Technology. Cham: Springer. DOI: 10.1007/978-3-030-29053-5.

Lusoli, Wainer et al. (2012). *Pan-European Survey of Practices, Attitudes and Policy Preferences as regards Personal Identity Data Management*. Scientific and Policy Report EUR 25295. Luxembourg. DOI: 10. 2791/81962.

Martí Sempere, Carlos (2011). “The European Security Industry: A Research Agenda”. In: *Defence and Peace Economics* 22.2, pp. 245–264. DOI: 10.1080/10242694.2011.542342.

Matzner, Tobias et al. (2016). “Do-It-Yourself Data Protection: Empowerment or Burden?” In: *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Ed. by Serge Gutwirth, Ronald Leenes, and Paul De Hert. Vol. 24. Law, Governance and Technology. Dordrecht: Springer, pp. 277–305.

Mokrosinska, Dorota (June 2017). “Privacy and Autonomy: On Some Misconceptions Concerning the Political Dimensions of Privacy”. In: *Law and Philosophy* 37.2, pp. 117–143. DOI: 10.1007/s10982-017- 9307-3.

Mordini, Emilio (2011). “Whole Body Imaging at airport checkpoints: the ethical and policy context”. In: *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*. Ed. by René von Schomberg. Luxembourg: Publications Office of the European Union, pp. 165–209.

Nielsen, Mathias Wullum et al. (April 30, 2018): *Ensuring Societal Readiness. A Thinking Tool*. Deliverable D6.1. NewHoRRIzon Project. URL: https://newhorrizon.eu/wp-content/uploads/2019/10/Deliverable_6.1_THINKING_TOOL.pdf

Nissenbaum, Helen (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

O’Neil, Cathy (2016). *Weapons of Math Destruction: How Big Data increases Inequality and threatens democracy*. New York: Crown Publishing.

Orlando, Domenico and Dewitte, Pierre (2019) “The ‘by design‘ turn in EU cybersecurity law: Emergence, challenges and ways forward“. In: *Security and Law*. Ed. by Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke, Cambridge, Intersentia.

Owen, Richard et al. (2012). “Responsible research and innovation: From science in society to science for society, with society”. In: *Science and Public Policy* 39.6, pp. 751-760. DOI: 10.1093/scipol/scs093

Pavone, Vincenzo, Sara Degli Esposti, and Elvira Santiago (Jan. 2015). *Key factors affecting public acceptance and acceptability of SOSTs*. Deliverable 2.4. SurPRISE project. URL: http://surprise-project. eu / wp - content / uploads / 2015 / 02 / SurPRISE - D24 - Key - Factors - affecting - public-acceptance-and-acceptability-of-SOSTs-c.pdf.

Pavone, Vincenzo et al. (2017). “Beyond the security paradox: Ten criteria for a socially informed security policy”. In: *Public Understanding of Science* 27.6, pp. 1–17. DOI: 10.1177/0963662517702321.

Regan, Priscilla M. (1995). *Legislating privacy: Technology, social values, and public policy*. Chapel Hill: University of North Carolina Press.

Rössler, Beate (2005). *The Value of Privacy*. Cambridge, Malden: Polity Press.

Spiekermann, Sarah (2016). *Ethical IT Innovation: A Value-Based System Design Approach*, Boca Raton: CRC Press.

Spindler, Mone et al., eds. (2020, in preparation). *Handbuch Integrierte Technikentwicklung. Zum interdisziplinären Einbezug ethischer, rechtlicher, sozialer und ökonomischer Aspekte in Technikentwicklungsprojekte* (Handbook integrated technology development: On the interdisciplinary inclusion of ethical, legal, social and economic aspects in technology development projects), Wiesbaden: Springer VS.

Steeves, Valerie M. (2009). “Reclaiming the social value of privacy”. In: *Lessons from the identity trail: anonymity, privacy, and identity in a networked society*. Ed. by Ian Kerr, Valerie M. Steeves, and Carole Lucock. Oxford; New York: Oxford University Press, pp. 191–208.

Stilgoe, Jack et al. (2013). “Developing a framework for responsible innovation”. In: *Research Policy* 42.9, pp. 1568-1580. DOI: 10.1016/j.respol.2013.05.008

Susser, Daniel, Beate Rössler, and Helen Nissenbaum (2019). “Technology, autonomy, and manipulation”. In: *Internet Policy Review* 8.2. DOI: 10.14763/2019.2.1410.

Taddeo, Mariarosaria (2019). “Is Cybersecurity a Public Good?” In: *Minds and Machines* 29.3, pp. 349–354. DOI: 10.1007/s11023-019-09507-5.

Valkenburg, Govert (2015). “Privacy versus security: problems and possibilities for the trade-off model”. In: *Reforming European Data Protection Law*. Ed. by Serge Gutwirth, Ronald Leenes, and Paul De Hert. Vol. 20. Law, Governance and Technology. Dordrecht: Springer, pp. 253–269. DOI: 10.1007/978-94-017- 9385-8.

Vallor, Shannon (2016). *Technology and the virtues : a philosophical guide to a future worth wanting*. Oxford and New York: Oxford University Press.

Van Enis, Quentin and de Terwangne, Cécile (2019), *L’Europe des droits de l’homme à l’heure d’Internet*, Brussels, Larcier.

van de Poel, Ibo (2019). “Core Values and Value Conflicts in Cybersecurity: beyond Privacy versus Security”. In: *The Ethics of Cybersecurity*. Ed. by Markus Christen, Bert Gordijn, and Michele Loi. Vol. 21. International Library of Ethics, Law and Technology. Cham: Springer. DOI: 10.1007/978-3-030- 29053-5.

van de Poel, Ibo and Lambèr Royakkers (2011). *Ethics, technology and engineering*. Oxford: Wiley-Blackwell.

van den Broek, Tijs et al. (2017). “Privacy and security: Citizens’ desires for an equal footing”. In: *Surveillance, Privacy and Security: Citizens’ Perspectives*. Ed. by Michael Friedewald et al. London: Routledge, pp. 15–35. ISBN: 9781138649248. DOI: 10.4324/9781315619309.

van den Hoven, Jeroen (2010). “The use of normative theories in computer ethics”. In: *The Cambridge Handbook of Information and Computer Ethics*. Ed. by Luciano Floridi. Cambridge: Cambridge University Press, pp. 59–76.

van der Sloot, Bart (2017). *Privacy as Virtue: Moving Beyond the Individual in the Age of Big Data*. Cambridge: Intersentia.

van Lieshout, Marc and David Barnard-Wills (July 17, 2015). *The PRISMS Decision Support System*. Deliverable 11.3. PRISMS project. URL: http://publica.fraunhofer.de/documents/N- 349845.html.

van Lieshout, Marc et al. (2014). “Reconciling privacy and security”. In: *Privacy and security in the digital age*. Ed. by Michael Friedewald and Ronald J. Pohoryles. London: Routledge, pp. 119–132.

von Schomberg, René (2014). “The quest for the ‘right’ impacts of science and technology: A framework for responsible research and innovation”. In: Responsible Innovation, Volume 1. Ed. by Jeroen van den Hoven et al. Dordrecht: Springer, pp. 33-50

Vrabel, Frantisek (Dec. 4, 2018). Presentation given at ”ICT 2018: Imagine Digital - Connect Europe”, Session on ”Tackling disinformation to support democracy”. Vienna. URL: https://ec.europa.eu/digital-single-market/events/cf/ict2018/item-display.cfm?id=21548.

Warren, Samuel D. and Louis D. Brandeis (1890). “The Right To Privacy”. In: *Harvard Law Review* 4.5, pp. 193–220.

Wenger, Florent et al. (Oct. 4, 2017). *Attitudes and Opinions Regarding Cybersecurity*. White Paper 3. CANVAS Project. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 3091920.

Westin, Alan F. (1967). *Privacy and freedom*. New York: Atheneum.

Yaghmaei, Emad et al. (Oct. 4, 2017). *Cybersecurity and Ethics*. White Paper 1. CANVAS Project. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091909.

Zedner, Lucia (2009). *Security*. Key ideas in criminology. London; New York: Routledge.

Zuboff, Shoshana (2019). *The Age of Surveillance Capitalism*. New York: PublicAffairs.

Zureik, Elia et al., eds. (2010). *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*. Montreal: McGill-Queen’s University Press.