UNIVERSITÉ DU LUXEMBOURG

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

PhD-FDEF-2023-012
The Faculty of Law, Economics and Finance

Department of Legal Studies

DISSERTATION

Defence held on 28/03/2023 in
Bologna to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG EN DROIT
and
DOTTORE DI RICERCA IN LAW, SCIENCE AND TECHNOLOGY

by

Pier Giorgio CHIARA
Born on 26 March 1994 in Turin (Italy)

SECURITY AND PRIVACY OF RESOURCE CONSTRAINED DEVICES

Dissertation defence committee

Dr Mark D. Cole, Dissertation Supervisor
Professor, Université du Luxembourg

Dr Raffaella Brighi, Disseration co-Supervisor
Associate Professor, Università di Bologna

Dr Vagelis Papakonstantinou, Chairman
Professor, Vrije Universiteit Brussel

Dr Dennis-Kenji Kipker, Vice Chairman
Professor, Universität Bremen

Dr Federico Costantini
Associate Professor, Università degli Studi di Udine

Alma Mater Studiorum – Università di Bologna
in cotutela con Università del Lussemburgo

DOTTORATO DI RICERCA IN

LAW, SCIENCE AND TECHNOLOGY

Ciclo XXXV°

Settore Concorsuale: 12/H3 – FILOSOFIA DEL DIRITTO

Settore Scientifico Disciplinare: IUS/20 – FILOSOFIA DEL DIRITTO

SECURITY AND PRIVACY OF RESOURCE CONSTRAINED DEVICES

Presentata da: Pier Giorgio Chiara

Coordinatore Dottorato
Prof.ssa Monica Palmirani

Supervisore
Prof. Mark D. Cole

Co-Supervisore
Prof.ssa Raffaella Brighi

Co-Supervisore
Prof. Ugo Pagallo
Università degli Studi di Torino

Esame finale anno 2023

Index:

Introduction

Problem Overview

A consensus on the definition of the Internet of Things (IoT) has not yet been reached. Yet, it is unlikely that a comprehensive overview of the huge and growing class of IoT hardware components can be drawn, since they are less standardised than hardware for personal computers. To make things more complex, the IoT brings together devices with limited CPU, memory and processing power, such as pressure sensors that require small, low-cost hardware to be economically competitive, and devices with powerful processors and large memories. As a result, the first class of devices – the *resource constrained devices* – does not have the necessary memory and computing power to run the most up-to-date and robust cryptographic protocols. Thus, research focuses on so-called "lightweight" cryptographic algorithms, which are more suitable for such constrained contexts. Like the IoT, the concept of resource-constrained devices remains vague as few technical taxonomies exist.

In the era of the Internet of Things, *security* and *privacy* are deeply intertwined. Manifold layers of complexity are under scrutiny. In a scenario where IoT devices physically interact with individuals, legal, ethical and technical aspects of the concepts of 'security', 'safety', 'privacy' and 'data protection' shall be considered, since they are intertwined more than ever before.

Enforceable cybersecurity rules require strengthening, to ensure both overall robustness and resilience against cyberattacks. Thus, IoT resource-constrained devices become not only global targets for direct attacks, but also assets for launching attacks. Existing and proposed horizontal and vertical, or sectorial, EU legislation does not address the challenges raised by unsecure IoT devices and related services at the core. The Directive (EU) 2016/1148 (NIS Directive) – the first piece of EU-wide legislation on cybersecurity – does not specifically and directly cover the IoT. Neither does Regulation (EU) 2019/881 (Cybersecurity Act), the most recent EU legal act covering ICT products and cybersecurity services. Therefore, the most recent initiatives of the Commission will be scrutinised and critically assessed against the backdrop of their potential impact on the field of IoT cybersecurity. These regard the massive revision of EU product safety legislation, the Proposal for a NIS2 Directive, and the yet-to-be-proposed Cyber Resilience Act as horizontal legislation on cybersecurity for connected products.

Furthermore, in order to secure the IoT environment, cybersecurity technologies are deployed to uphold individuals' rights to privacy and protection of personal data. However, a closer look reveals

that the enjoyment of these fundamental rights may be paradoxically jeopardised by these technologies, as they increase the attack surface and therefore introduce new vulnerabilities. Structural IoT data and metadata harvesting, processing and sharing triggers and challenges specific aspects of the EU privacy and data protection law, such as the notions of consent, transparency and profiling.

Finally, ENISA already pointed out that, as there is no common EU-wide approach to addressing the cybersecurity risk in IoT, or a common multi-stakeholder model, most companies and manufacturers are taking their own approach when implementing security, resulting in a lack of or slow embracement of standards to guide the adoption of IoT security measures and good practices[1]. When considering the gaps affecting the Single Market in the field of (IoT) cybersecurity, the lack of interoperable solutions (i.e., technical standards) is certainly the thorniest obstacle that may still hinder IoT from its full realisation. In the 2021 Rolling Plan for ICT Standardisation, the EU Commission noticed that "a large number of proprietary or semi-closed solutions to address specific problems have emerged, leading to non-interoperable concepts, based on different architectures and protocols. Consequently, the deployment of truly IoT applications, i.e., where information of connectable 'things' can be flexibly aggregated and scaled, has been limited to a set of 'intranets of things — or goods'"[2].

To make things more complex, with regard to the risk to fundamental rights, in particular, the right to privacy and the right to the protection of personal data, existing Data Protection Impact Assessments (DPIA), under Art. 35 of Regulation (EU) 2016/679 (GDPR), consider technical security measures to be a part of the controls that the methodology needs to take into account. In turn, traditional risk analysis models in the field of information security acknowledge privacy and data protection requirements as sub-sets of the overall process. The hiatus boils down to the rationale of the two assessments: the former aims at safeguarding individuals' *fundamental rights and freedoms*; the latter considers *the assets of the organisation* evaluating the risk from a security standpoint.

A holistic risk analysis methodology for the IoT, aiming at combining the two aspects, should encompass the full breadth and depth of 'security and privacy' considerations to tackle, therefore eschewing the horizon of an 'Internet-of-insecure-things'. In the words of EU Commission President von der Leyen, at the 2021 State of the Union Address, "if everything is connected, everything can be hacked. Given that resources are scarce, we have to bundle our forces. And we should not just be

[1] ENISA, 'Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures' (2017) 53 <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>.

[2] European Commission, 'Rolling Plan for ICT Standardisation 2021' (2021) 30.

satisfied to address the cyber threat, but also strive to become a leader in cybersecurity". Cybersecurity has become one of the most urgent issues of our days. It is not only a pre-condition for individuals' safety and fundamentals rights, but it is also necessary to uphold the critical infrastructure, the economy and national security. In other words, it is essential to preserve democracy.

Methodology

The research is driven by three core objectives, set by the H2020-MSCA-ITN Grant Agreement no. 814177:

I) Analysis of the weaknesses of resource-constrained IoT devices;
II) Analysis of legal frameworks regulating IoT security;
III) Security framework and best practices for resource-constrained devices.

Accordingly, this study aims to shed light, from a legal, ethical and technical perspective, on the following main research question:

To what extent does existing EU cybersecurity and data protection legislation provide manufacturers of IoT resource-constrained devices with obligations and legal certainty vis-à-vis 'security and privacy' aspects and foster consumers' trust?

Each chapter considers different sub-questions that ought to guide the research:

I) What can a functional and working definition of IoT, and resource-constrained devices particularly, be? What is the relationship between these concepts? To what extent does a traditional threat taxonomy fit the IoT domain?
II) What are the different meanings and values of "security" in the IoT era? To what extent are security and safety intertwined with privacy and data protection in IoT?
III) To what extent does the selected EU legislation on cybersecurity take into account the IoT? What are the obligations of IoT manufacturers in relation to cybersecurity requirements? What models of governance are best suited to addressing IoT security challenges? To what extent could the proposed horizontal legislative measures on cybersecurity for connected devices improve the standard of protection for the IoT?
IV) What are the legal challenges brought about by IoT cybersecurity to the fundamental rights to privacy and protection of personal data? Taking encryption as an interface of the privacy-security debate, how can a fair balance between the different interests be achieved?

V) How can we holistically assess safety, cybersecurity, privacy and data protection risks in the IoT while upholding a fundamental rights perspective?

The methodology consists of an interdisciplinary literature review, integrating legal, philosophical, and technical reflections. The literature analysis that underpins this study involved searching several databases, such as Google Scholar, Scopus, SSRN and IEEE, from October 2019. In this respect, for the sake of fairness and transparency, it should be acknowledged that the core ideas underlying this work may have been published in scientific articles by the author of this thesis, albeit from different angles. The desk research builds on relevant documents, among which, EU laws, EU publications, and academic publications, as well as positioning papers both of consumer and industry associations.

The underlying hope of this research is to substantiate the strong statement of the c.a.s.e. collective's manifesto with respect to research in the field of "security" in Europe: "the goal of a critical intellectual is not only to observe, but also to actively open spaces of discussion and political action, as well as to provide the analytical tools, concepts and categories for possible alternative discourses and practices"[3]. Thus, following the critical approach of the Frankfurt School' philosophers[4], this interdisciplinary research aims at examining the (relevant and applicable) law in its dependence on society, that is, the philosophical and technical context where the legal framework lies[5], to assess the impacts it has on the background it regulates. The inclusion of ethics ensures the alignment of security research and development with principles like fundamental rights[6], such as data protection and privacy, and democracy, "instead of quelling these in the name of security"[7].

[3] C.A.S.E. Collective, 'Critical Approaches to Security in Europe: A Networked Manifesto' (2006) 37 Security Dialogue 443, 476 <https://journals.sagepub.com/doi/10.1177/0967010606073085> accessed 19 October 2021.

[4] Max Horkheimer, *Critical Theory: Selected Essays* (Matthew O'Connell (translated by) ed, The Continuum Publishing Company 2002) 188–243 <https://monoskop.org/images/7/74/Horkheimer_Max_Critical_Theory_Selected_Essays_2002.pdf> accessed 19 October 2021; Max Horkheimer and Theodor W Adorno, *Dialectic of Enlightenment: Philosophical Fragments* (Gunzelin Schmid Noerr and Edmund Jephcott (translated by) eds, Stanford University Press 2002).

[5] Walter Benjamin, *Walter Benjamin: Selected Writings, 1: 1913-1926* (Marcus Paul Bullock and Michael William Jennings eds, Harvard University Press 2004) 251 <http://www.riss.kr/link?id=M12705986> accessed 19 October 2021: in its critique of violence, Benjamin states that it is "the philosophy of its history – […] because only the idea of its development makes possible a critical, discriminating, and decisive approach to its temporal data". Notwithstanding, the abovementioned quote should not be understood as a methodological commitment to the legal dialectic highlighted by Benjamin in terms of law-making – law-preserving.

[6] Nicola Stingelin and others, 'Roles and Functions of Ethics Advisors/Ethics Advisory Boards in EC-Funded Projects' (2012) 3 <https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/ethics-guide-advisors_en.pdf> accessed 12 October 2021.

[7] Matthias Leese, Kristoffer Lidén and Blagovesta Nikolova, 'Putting Critique to Work: Ethics in EU Security Research' (2019) 50 Security Dialogue 59, 63 <https://doi.org/10.1177/0967010618809554>.

The complexity of today's legal and technical challenges on IoT regulation calls for a careful balance of top-down and bottom-up approaches[8]. In recent discussions within the Council of the European Union, Member States acknowledge that a more cross-disciplinary and comprehensive approach is needed in tackling the challenges raised by new technologies[9]. Therefore, the legal analysis of Chapter 3 will shed light both on hard law and soft law legal instruments. The focus will be shifted from a traditional conceptualisation of the law, adhering to a top-down approach, such as the NIS Directive, to co-regulation, such as the Cybersecurity Act or EU product safety legislation, where harmonised technical standards developed by European standardisation organisations are used to demonstrate the conformity of certain products or services with the legal (essential) requirements enshrined in the legal acts. In order to avoid broadening the scope of the analysis too extensively, sectorial legislation will be analysed only to the extent that cybersecurity requirements for IoT systems are introduced. The resulting model will provide a clear overview of the EU legal landscape applicable in the context of IoT cybersecurity.

Finally, the rationale behind the order of the chapters follows the traditional paradigm of security & privacy information security risk management. 'Risk' is unavoidably the *fil rouge* of this work. In this respect, it is worth mentioning that we are not committing ourselves to the information security approach from a methodological viewpoint. Rather, information security's core components, namely vulnerabilities – threats – risks, will be extrapolated and assessed using an interdisciplinary method that takes into account not only the technical aspects of security, but also the legal and philosophical ones. For instance, vulnerabilities are analysed from a twofold perspective. Chapter 1 delves into resource constrained devices' vulnerabilities – or weaknesses – from a technical standpoint, culminating in a critical analysis of the IoT threat taxonomy model of ENISA, whereas Chapter 4 explores them from a data protection and privacy perspective. Taking into account the resulting combination thereof, a holistic risk analysis methodology will be introduced in Chapter 5, with a view to mitigating cybersecurity and data protection risks, by taking into account specific IoT threat and vulnerability scenarios.

In the field of cybersecurity, the so-called 'holistic approach' is increasingly gaining ground. When managing the cybersecurity risk, traditional information security methods are no longer sufficient to

[8] Ugo Pagallo, Pompeu Casanovas and Robert Madelin, 'The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data' (2019) 7 Theory and Practice of Legislation 1; Monica Palmirani and Michele Martoni, 'Big Data, Governance Dei Dati e Nuove Vulnerabilità' (2019) 35 Notizie di Politeia 9.

[9] Council of the European Union, 'Preparation of the Council Position on the Evaluation and Review of the General Data Protection Regulation (GDPR) - Comments from Member States 12756/1/19 REV 1' (2019) <https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf>.

counteract the rapidly evolving threat landscape. In this respect, other factors are increasingly taken into consideration: addressing the 'human factor', that is, promoting cybersecurity awareness either in public or private entities, fostering education and 'cyber hygiene' good practices; strengthening cooperation and information sharing among stakeholders; pursuing strategic autonomy through public-private partnerships; enhancing cyber resilience in order to survive disruptive attacks.

In line with the methods and outcomes of the Deliverable *D4.1 – Risk Analysis of Different IoT Devices* of the LAST-JD-RIoE project, with the MSCA ITN EJD Grant Agreement no. 814177, drafted by the author of this thesis, the holistic approach is understood to be an attempt to reconcile two different rationales: the safeguarding of fundamental rights and freedoms, that is, the GDPR perspective, and the traditional information security assets-driven standpoint. If we were to accept the *infraethical* premise presented in Chapter 2, the traditional approach of information security, aiming at protecting the assets of the organisation, is compatible with the GDPR approach, which aims to protect individuals' fundamental rights and freedoms. One caveat applies: the fundamental rights perspective must be at the core of the assessment. The security of IoT systems architecture and supply chain is prodromal to safeguarding individuals' safety and fundamental rights. To confirm the validity of such understanding, from an operational standpoint, it could be observed that the roles leading these assessments i.e., the data protection officer (DPO) and the chief information security officer (CISO), often converge in the same person or are at least carried out within the same team.

Against this background, Chapter 5 – dedicated to the holistic risk assessment, addresses the outcomes of the French Data Protection Authority (CNIL) methodology for an IoT data protection impact assessment (DPIA). The reasons behind this choice are twofold. First, to the author's knowledge, the CNIL DPIA model for IoT devices is the first attempt by a public authority to define a methodology for managing the privacy & data protection risk specifically within the IoT domain. Second, the flexibility of the methodology enables integration with established and successful methodologies in the field of cybersecurity, thus leaving room for realisation of the holistic approach.

Description of the Work

Chapter 1 aims at providing a functional and sufficiently comprehensive definition of the 'IoT'. The analysis sheds light on i) the architecture taxonomy of IoT systems; ii) the so-called IoT verticals, that is, the application domains; iii) the blurred concept of "resource-constrained" devices; and, iv) the IoT security threat taxonomy.

The architecture taxonomy of the IoT results in a 3-layer model which aims to combine an overview of the technical components with the corresponding data collection, processing and sharing. The first

layer of the model is the so-called device level, which considers the "things" in IoT. The second layer, that is, the network level, illustrates how IoT components *communicate* within the Internet infrastructure. Finally, the application layer aims at assuring abstraction across the manifold devices and sources of data. In other words, it is responsible for monitoring and controlling IoT elements in the IoT device and network layers.

As the aim of this work is to provide a cross-sectorial overview of the main security and privacy risks connected to IoT devices, the section on the IoT verticals will not dwell extensively on the various and diverse requirements of the many application domains. Rather, the most significant application domains are presented to highlight the relevance of the IoT paradigm vis-à-vis the EU single market and society at large. The chosen domains are the ones covered by the EU IoT Large-Scale Pilot projects: eHealth, Smart Farming, Smart Homes, Smart Cities, Smart Vehicles.

The third section of Chapter 1 elaborates the notion of 'resource constraints'. The IoT ecosystem is going to be increasingly made up of *constrained* connected devices. Without delving into a classification of resource-constrained devices from a purely technical perspective, this work relies on the assumption that IoT environments always involve constrained technologies in terms of computational power, regardless of potentially non-constrained technologies embedded in the system. The IoT combines multiple technologies, such as radio-frequency identification (RFID), wireless sensor networks, cloud computing and fog computing, which span a large spectrum of computational power. Therefore, each of these technologies has its own security requirements and privacy concerns. The major challenge is that one must secure the chain of all those technologies, as the cybersecurity robustness of an IoT system will be judged based on its weakest point, its 'Achilles' heel'. Thus, this section introduces the issue of cryptography – one recurring theme of this work, as a prominent interface between *security* and *privacy* – in particular, having regard to the application of 'lightweight encryption' to resource-constrained devices, which involves trade-offs between performance and security.

The last section accounts for an IoT threat taxonomy by integrating the ENISA report on IoT threat taxonomy with the more encompassing ENISA 2020 threat landscape. The goal is to focus on IoT vulnerabilities not only at device level, but also taking into account the related network and internet-connecting aspects. The so-called threat landscape has been classified in relation to the consequences the attack scenarios pose either to the system, such as service compromising and sensing domain attacks or to the underlying data sharing, such as packets crafting, packets alteration, and traffic analysis, whose legal effects will be further addressed in Chapter 4. The traditional concept of establishing a security perimeter i.e., setting up the essential equipment and technologies to prevent

an outside attack against a network, became quite outdated with the advent of ubiquitous IoT. As mentioned in the previous section, the IoT architecture not only amplifies the surface of the perimeter disproportionately, but also the compelling need to secure the supply chain across the IoT ecosystem would make the identification of a perimeter impossible. The guidelines issued by ENISA for securing the IoT supply chain, where each recommendation contains related good practices and relevant standards, are critically analysed in order to assess the consistency with the holistic approach of this work.

Chapter 2 aims to disentangle the 'security debate' from a normative perspective. Through a doctrinal literature review, the resulting theoretical framework will serve as a solid foundation for the legal analysis of the EU legal framework regulating IoT security that follows in Chapter 3.

The first part of the reflection delves into the scope and rationale of the blurred concept of 'cybersecurity'. With technological evolution and increasing digitalisation, the paradigms of information security have changed to the point of converging in the concept – broad and transversal to different disciplines – of cybersecurity. It is often used interchangeably with the more established terms *computer* or *information security*. Whereas they aim at common goals – to increase the level of security in the cyberspace and withstand attacks, information security only represents a subset of cybersecurity. In a landscape of complex interaction between information systems, society and the environment, cybersecurity broadens the perimeter of the risks and actors involved with the consequent identification of new elements of protection.

Furthermore, cybersecurity is relevant not only as a value *per se*, in the sense of a fundamental good worth of protection. It also needs to be protected in view of national security, the protection of critical infrastructures, the development of the digital market and the enjoyment of fundamental rights and freedoms by individuals. This instrumental perspective lays a solid foundation for a normative theoretical framework which would treat cybersecurity – in its sole dimension of systems' robustness – as a public good to be managed in the public interest. On the one hand, robust and secure systems foster trust in the digital environment; on the other hand, this dimension of cybersecurity facilitates the promotion of fundamental rights and freedoms, such as the right to privacy and the protection of personal data, freedom of expression and information. Conversely, resilience – understood in the dimension of threat detection – imposes a delicate balance between the desired degree of security and fundamental rights, such as the right to privacy and data protection. Similarly, facilitating responsiveness may not lead to a global and collective improvement of cybersecurity. On the contrary, it is likely to lead to an intensification of cyberattacks. When it becomes necessary to weigh *cybersecurity-as-a-fundamental-good,* as in the cases of resilience and responsiveness, and other

fundamental goods, such as privacy, 'bad ethics' apply trade-offs rather than balances. For the latter suggests that the more intensive the infringement of fundamental rights, the more effective safeguards must be implemented, according to the framework and traditions of the European Court of Justice and European Court of Human Rights.

All in all, to achieve a high level of protection, in the face of increasingly transnational challenges and threats, the European Union promotes a global strategic approach, based on international cooperation and the sharing of information at all levels, redistributing responsibilities between the public and private sectors. Even citizens shall assume a certain degree of responsibility for stimulating conscious behaviour. It is therefore necessary for all organisations to adopt *holistic* paradigms for cybersecurity that promote awareness of compliance requirements for products, services and processes, in order to ensure appropriate levels of risk management in an increasingly diverse and complex environment.

Lastly, the instrumental and fundamental understandings of 'security' might be better appreciated through the crucial distinction between the intertwined concepts of *safety* and *security* which are sometimes used interchangeably – especially in the context of IoT. The paradigm shift brought by IoT, bridging the physical and cyber-environment, may suggest addressing traditional notions of security and safety in a 'unified' way or more interchangeably. Nonetheless, these conceptual distinctions must be kept firm, to build a clear and coherent regulatory framework vis-à-vis EU safety and (cyber)security legislation, to which the following chapter is dedicated.

Chapter 3 maps out the different legal frameworks regulating 'IoT security' in the EU. After a brief overview of the evolution of the concept of cybersecurity in Union policy, the investigation first considers Directive EU 2016/1148 on security of network and information systems (NIS Directive), the first piece of European legislation on cybersecurity, which does not specifically and directly address the IoT. The legal analysis highlights the extent to which the current normative architecture of the NIS, which builds upon the distinction between Operators of Essential Services and Digital Service Providers, encompasses IoT cybersecurity and whether regulatory gaps exist. In particular, two different issues are under scrutiny: (i) the risk of legal fragmentation that can result from the potential overlap of cybersecurity and incident notification requirements between the NIS Directive and other existing breach reporting duties under EU legislation, such as the GDPR or the European Electronic Communications Code (EECC); and (ii) the exemption of hardware manufacturers and software developers.

The legal analysis then considers the European framework for cybersecurity certification of ICT products, services and processes introduced by Regulation (EU) 2019/881 (the Cybersecurity Act) as

an important part of the ongoing European Commission programme for strengthening the Union's digital security. On the one hand, manufacturers, developers and vendors of ICT products, services and processes can rely on scalable and granular schemes to assess whether the specific security controls and measures of their technological solutions comply with specified security requirements. On the other hand, consumers and citizens are offered information on the level of security of certified ICT assets in a transparent manner. The question is whether the Cybersecurity Act could eventually fill significant regulatory gaps and inconsistencies in the EU cybersecurity legal framework, notably the NIS Directive, in particular, regarding manufacturers and developers' lack of legal obligations vis-à-vis the cybersecurity of their technological solutions.

Against this background, the Commission's approach vis-à-vis the ever-growing number of unsecure IoT devices in the Single Market consisted of revising different legal acts within EU product safety legislation to include essential cybersecurity requirements. Accordingly, the analysis focuses on several pieces of legislation which show, albeit from different angles, how cybersecurity is progressively linked to the safety regulation of (connected) products. These are: the Radio Equipment Directive (RED) and the Delegated Act activating the essential requirements under Article 3(3)(d), (e) and (f) RED, the Medical Devices Regulation, the Proposal for a Machinery Regulation and the Proposal for a General Product Safety Regulation. Overall, product safety legislation is primarily concerned with the design and manufacturing phases, which are linked to the placing and making available of products on the market, whereas cybersecurity – and IoT specifically – requires dynamic risk management, that must be ensured throughout the entire life cycle of the devices. Thus, the inclusion of cybersecurity requirements in such sectoral legislation is questioned – if not openly opposed – by many stakeholders, arguing that the Commission has embarked upon a path towards fragmented and contradictory legal requirements. Although a sectoral approach to the issue of connected products security may prove to be effective in the short term, only horizontal legislation seems to be able to address the problem at the core in the most efficient way, as shown in the last section of Chapter 3.

In further parts of the thesis, the proposal for a NIS2 Directive – which seeks to modernise the existing legal framework and addresses several weaknesses that prevented the existing Directive from unlocking its full potential – is scrutinised, with regard to the extent to which it would address the complexity raised by the IoT ecosystem. In particular, the analysis aims at testing whether and to what extent the revised NIS Directive would ensure a higher standard of protection against unsecure IoT devices by taking into account and addressing the following issues: i) the enlarged scope of the

NIS2, in particular, taking into account the 'manufacturing' sector; ii) the vulnerability disclosure and handling procedures; and, iii) new cybersecurity requirements for the supply chain.

The legislative gap analysis of EU laws related to cybersecurity for connected (IoT) devices carried out in the previous sections of Chapter 3 highlights a fragmented regulatory framework that does not specifically and comprehensively tackle the problem of a Single Market flooded by unsecure connected products. Therefore, the last section casts light on the core regulatory drivers underpinning the announced Cyber Resilience Act (CRA). These are: mandatory cybersecurity essential requirements for all connected digital products and ancillary services; reference to European harmonised technical standards and conformity assessment; effective market surveillance. In order to avoid duplicate requirements and thus legal fragmentation, the CRA needs to be streamlined and aligned with the most recent initiatives undertaken by the Commission in order to close some gaps concerning the cybersecurity of digital products, as addressed in Chapter 3.

The legal analysis of Chapter 4 casts light on three normative challenges in terms of fundamental rights, in particular, the right to privacy and the right to the protection of personal data (Arts. 7 and 8 of the EU Charter of Fundamental Rights), brought about by the structural data and metadata sharing of the ubiquitous IoT. The first legal challenge concerns the realignment of the traditional matters of privacy and data protection, which can be observed under IoT data and metadata sharing. When it comes to mapping the privacy debate on the IoT, it is often hard to discern the right to privacy-related issues from data protection ones. Indeed, software engineering literature, or more generically the *technical community* as opposed to the *legal* one, tends to acknowledge privacy in a holistic fashion, that is to include data protection related concerns without making a due and appropriate division. The danger of this trend, which is especially rooted in non-EU legal frameworks (e.g., the US), is that the incorrect framing of the problem might lead to legal uncertainty and thus prevent the single market from functioning properly. Therefore, the first section of the Chapter explores how structural data and metadata processing and sharing of the IoT challenges the two different regimes of the ePrivacy Directive and the GDPR, in particular, taking into account the broad concept of 'personal data'.

The second legal challenge casts light on the relationship between various cryptographic technical tools, regarding, but not limited to, encryption, and the traditional legal disciplines of privacy and data protection. Thus, an alignment of privacy, data protection and *cybersecurity* – to be understood broadly to cover information security (see Chapter 2) – is particularly striking when it comes to cryptographic technologies which aim to ensure confidentiality in the processing process, in particular, concerning data sharing and network communication. Firstly, the analysis sheds light on the rationale of encryption, which differs substantially from hashing and pseudonymisation, albeit the

latter is generally achieved by means of cryptography, and why this distinction matters when it comes to upholding the fundamental rights to privacy and data protection. The legal analysis focuses on whether and to what extent state-of-the-art encryption protocols challenge the already blurred distinction between personal and non-personal data that underlies the EU data protection legal framework. Finally, the discussion considers the often-overlooked impact of encryption on *privacy*, in terms of infringement of the fundamental right it aims to protect.

Notwithstanding the lightweight – in the case of resource-constrained devices – or 'strong' encryption protocols that may be adopted to secure (IoT) device communication, serious privacy concerns nevertheless arise as an adversary can gather user activity-related inferences by relying on some metadata properties accompanying the encrypted data. Thus, encrypted traffic analysis, or rather, metadata analysis, that corresponds to the third legal challenge is definitely a current and important topic in the search for securing IoT users' privacy. Against the background of the remaining three legal issues identified by the Article 29 Working Party in its Opinion on the IoT, the final section of Chapter 4 firstly casts a technical light on state-of-the-art attacks and techniques used for eavesdropping on encrypted traffic, enabling granular profiling and surveillance of habits and behavioural patterns. It then addresses the relevant existing and future European privacy legal frameworks that can tackle the above-mentioned challenges, in particular regarding device fingerprinting. The legal analysis specifically demonstrates that the long-awaited ePrivacy Regulation would strengthen and enhance users' privacy protection with particular regard to passive network analysis and notably including device fingerprinting, even if some aspects of Art. 8 of the ePrivacy Regulation Proposal would still need further clarification from the co-legislators.

Chapter 5 focuses on how to assess the IoT '*security* and *privacy'* risks in IoT systems. Risk assessment is one of the core elements into which the cybersecurity and privacy & data protection EU legal frameworks are clustered.

In particular, the first section of the chapter lays out the different rationales of traditional information security risk management models (e.g., ISO framework) and the fundamental rights-based model of the GDPR data protection impact assessment (DPIA) enshrined in Art. 35, in order to identify misalignments and potential synergies between the two frameworks. The *infraethical* perspective (Chapter 2) aims at clarifying the relationship between the two: cybersecurity technical and organisational measures must facilitate data protection and privacy principles to uphold individuals' rights and freedoms. In line with the holistic methodological approach outlined in the methods section, risk assessment methodologies should go beyond the limited perspective adopted in today's

DPIA methodologies, which mainly revolve around data quality and data security, to encompass a broader set of fundamental rights and freedoms (as *per* Art. 35 GDPR).

Against this background, the data protection impact assessment (DPIA) developed by the French Data Protection Authority (CNIL) for IoT devices is critically analysed to investigate whether and to what extent the methodology assesses the risks to individuals' rights and freedoms in the specific context of IoT devices. *Prima facie,* the French DPA's approach is in line with the above-mentioned *infraethical* understanding, as it embeds several security controls by 'EBIOS risk manager' i.e., the method for assessing and treating digital risks, published by the French National Cybersecurity Agency (ANSSI). However, feared events that ought to be considered by the risk assessment should not be limited to the CIA triad (confidentiality, integrity and availability) but will encompass a broader range of cybersecurity objectives. In this regard, Art. 51 of the Cybersecurity Act may provide a legitimate basis when identifying such objectives.

Moreover, CNIL DPIA for IoT devices seemingly fails to adopt a *holistic* approach to the safeguarding of 'rights and freedoms', by only focusing on selected aspects of data security which may impact the fundamental rights to privacy and personal data protection. Hence, the last section of Chapter 5 presents a holistic data protection impact assessment model for IoT devices with the view to integrate CNIL IoT DPIA i) with the cybersecurity objectives of Art. 51 Cybersecurity Act; and, ii) with a broader scope of the diverse fundamental rights that may be impacted by IoT systems.

Chapter 1. The Internet of Things

Although the first defining attempts date back to the late 1990s[10], it is challenging today to provide an all-encompassing definition of the Internet of Things, widely known by its acronym "IoT", given its technical and structural complexity. Yet, a solid consensus has been built up around its twofold constitutive nature: an enabling technology and a global infrastructure for connecting the physical and the virtual worlds[11].

On the one hand, according to ISO/IEC, the IoT is the revolutionary "enabling technology that consists of many supporting technologies"[12], to name a few, information and communication networking technologies (e.g., cloud computing, fog computing, edge computing, 5G), sensing and connecting technologies (e.g., wireless sensor networks, radio-frequency identification (RFID), Bluetooth, GPS), software technologies (e.g., artificial intelligence), and device/hardware technologies. Each of these technologies has its own vulnerabilities: the ultimate challenge of IoT security is securing the chain of all those technologies as the security resistance of an IoT application will be judged based on its weakest point which is usually referred to as its Achilles' heel[13]. On the other hand, the IoT is a network of "things", embedded with software intelligence, which are connected to the Internet[14]. In order to unravel the definition, it is worthwhile decoupling the most generic components which enable this network of "things": sensors, to collect data in the environment nearby; actuators, to act upon said environment; identifiers, to identify data sources; and, software elements, to process data.

It is worth clarifying from the outset the relationship between the IoT and cyber-physical systems (CPS), which integrates computational and physical processes, to dispel any ambiguity which still gives rise to speculation about the scope of these concepts. The U.S. National Institution of Standards

[10] Kevin Ashton "invented" the term "IoT" in a presentation delivered at Procter & Gamble in 1999 concerning the integration of RFID technology in the supply chain of P&G. The definition gained momentum and was resumed by MIT (2001) and later by ITU (2005).

[11] Stefano Nativi, Alexander Kotsev and Petra Scudo, *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins) A Multi-Facets Analysis* (Publications Office of the European Union 2020) 10 <https://ec.europa.eu/jrc> accessed 20 September 2021.

[12] ISO/IEC, 'ISO/IEC 30141:2018(En), Internet of Things (LoT) — Reference Architecture' (2018) <https://www.iso.org/obp/ui/es/#iso:std:iso-iec:30141:ed-1:v1:en> accessed 20 September 2021.

[13] Ammar Rayes and Samer Salam, *Internet of Things From Hype to Reality* (Springer 2019) 235; Elisa Bertino, 'Security and Privacy in the IoT', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Springer Verlag 2018) 8.

[14] Rayes and Salam (n 13) 2.

and Technology (NIST) defines cyber-physical systems as "smart systems that include engineered interacting networks of physical and computational components"[15]. Given the above-mentioned provisional definitions of IoT, it makes sense to conclude that both CPS and IoT can be subsumed under the broader category of digital Information Communication Technologies (ICTs).

Marwedel noted that, "[t]o some extent, it is a matter of preferences whether the linking of physical objects to the cyber-world is called CPS or IoT. Taken together, CPS and IoT include most of the future applications of IT"[16]. Such understanding of these concepts is reflected in the words of Denardis, who believes that the term CPS, albeit imperfect, is better suited to describe "this phenomenon of blurring physical and digital domains, simply because IoT, over time, has in popular discourse become synonymous with consumer markets, thereby obfuscating the larger phenomenon of embedded devices in critical sectors including agriculture, defense, transportation, and manufacturing"[17].

For the purpose of this work, the term IoT will be preferred to CPS, as legislative texts and legal doctrine increasingly rely on it when referring to the next generation of embedded and interconnected ICTs systems.

The pervasive, or ubiquitous, multi-purpose and multi-device computing brought about by the IoT is indeed leading to a paradigm shift, which is a major evolutionary step in Internet history. "Similar to how the inception of the World Wide Web transformed access to knowledge and spurred entirely new industries, cyber-physical systems are now similarly transformational"[18]. Thus, some prefer the term Internet of Everything (IoE)[19], as it brings together things, processes, people – as end-nodes of this network – and data, both related to the environment and the individuals[20]. Regardless of the various

---

[15] NIST, 'Framework for Cyber-Physical Systems Release 1.0' (2016) xiii.

[16] Peter Marwedel, *Embedded System Design: Embedded Systems Foundations OfCyber-Physical Systems, and The-Internet OfThings* (Fourth, Springer 2021), 4.

[17] Laura Denardis, *The Internet in Everything - Freedom and Security in a World with No Off Switch*, vol 148 (1st edn, Yale University Press 2020) 27–28.

[18] ibid 26. Against the background of the contextual heterogeneity of these systems, Denardis proposes a fourfold taxonomy which aims to unveil common technical characteristics: (1) the digitisation of everyday objects, including consumer IoT devices and objects connected in municipalities; (2) the Internet of Self, which includes objects in close proximity to the body, such as wearable technologies and digitally connected medical devices; (3) the industrial Internet of Things or "Fourth Industrial Revolution," a term that captures the cyber-embeddedness of objects in industrial sectors; and (4) emergent cyber-physical systems, which include material objects that are born digital, such as additive manufacturing (also called 3D printing), robotics, and augmented reality.

[19] CISCO, 'The Internet of Everything - Global Public Sector Economic Analysis ' (2013).

[20] Jacopo Iannacci, 'Internet of Things (IoT); Internet of Everything (IoE); Tactile Internet; 5G – A (Not so Evanescent) Unifying Vision Empowered by EH-MEMS (Energy Harvesting MEMS) and RF-MEMS (Radio Frequency MEMS)' (2018) 272 Sensors and Actuators, A: Physical 187.

classificatory attempts, the IoT is the next step of the transformation of Internet, as it deals with technologies, processes, people and massive real-life interactions.

Whether one uses the term "Internet of Everything" or "Internet of things" or "embedded systems" or "cyber-physical systems" or "network of everything" is not as important as acknowledging the very real underlying technological transformation—the fundamental integration of material-world systems and digital systems[21].

In other words, an ecosystem where everyone and everything is connected. From an epistemological viewpoint, IoT ubiquitous computing renders the physical – virtual dichotomy rather anachronistic, as, in the words of Floridi,

"we no longer live online or offline but onlife, that is, we increasingly live in that special space, or infosphere, that is seamlessly analogue and digital, offline and online. If this seems confusing, perhaps an analogy may help to convey the point. Imagine someone asks whether the water is sweet or salty in the estuary where the river meets the sea. Clearly, that someone has not understood the special nature of the place. Our mature information societies are growing in such a new, liminal place, like mangroves flourishing in brackish water. And in these 'mangrove societies', machine-readable data, new forms of smart agency and onlife interactions are constantly evolving, because our technologies are perfectly fit to take advantage of such a new environment, often as the only real natives"[22].

To conclude, an all-encompassing, high-level definition of the 'IoT' summing up the elements described above could be the one recently provided by the European Commission in its proposal for a Data Act. In recital 14, the Internet of Things – covered by the proposed Regulation – is referred to as "physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service". Interestingly, this definition is incorporated in the definition of 'product' generally[23], confirming therefore the *onlife* paradigm.

1.1 The IoT Architecture Taxonomy

The three-layered architecture of IoT presented below builds on Rayes and Salam's[24] taxonomy: due to its straightforward configuration, it appears to be the best suited to fulfil the goal of the present

[21] Denardis (n 17) 28.

[22] Luciano Floridi, 'Soft Ethics and the Governance of the Digital' (2018) 31 Philosophy & Technology 2018 31:1 1, 1.

[23] Art. 2, point 2, Data Act proposal.

[24] Rayes and Salam (n 13).

Chapter, that is, to provide the clearest possible overview of a reference model for the IoT. Yet, this taxonomy can be compared and combined with other existing IoT architectures, such as the one of the European Network and Information Security Agency (ENISA)[25], International Telecommunication Union (ITU)[26], Alliance for the Internet of Things Innovation (AIOTI)[27], US National Institute of Standards and Technology (NIST)[28] and International Standardisation Organization (ISO)[29]. All in all, these high-level models are composed of several layers of abstraction, from the three layers of AIOTI, through the four of ENISA and ITU, to the five of NIST and the six of ISO/IEC. The three-layer model that follows serves to systematically identify and break down the IoT into its core components in light of the analysis of security threats to these assets of section 1.4.

1.1.1 The device layer

The first layer of the IoT architecture i.e., the device layer, considers the "things" in IoT. Sensing, actuating and unique identification are the three key requirements for this level[30]. Sensors are the starting point in IoT data collection: they are electronic embedded devices that *sense* the surrounding environment. In other words, they provide a usable output, defined as an electrical quantity, in response to a specified measurand, a physical quantity or a property[31].

In this respect, three classes of issues arise: emission or transduction, as regards the generation of electromagnetic signals; susceptibility, as the tendency to break down under unwanted emissions[32]; coupling, which refers to how the emitted interference reaches some target device[33]. Apart from sensors, RFID and video tracking are two classical technologies through which the surrounding environment is captured and monitored. The former is a mechanism to capture information pre-embedded into the so-called "tag" of a thing or an object using radio waves through a "reader"; the latter is the process of capturing and analysing the video feeds, frame by frame, of a particular object

[25] ENISA, 'Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures' (n 1).

[26] ITU-T, 'Overview of the Internet of Things', vol 6 (2012).

[27] AIOTI, 'High Level Architecture (HLA) AIOTI WG03-LoT Standardisation' (2018).

[28] Jeffrey Voas, 'NIST Special Publication 800-183 Networks of "Things"' (2016) <http://dx.doi.org/10.6028/NIST.SP.800-183> accessed 22 September 2021.

[29] ISO/IEC, 'ISO/IEC 30141:2016 Information Technology-Internet of Things Reference Architecture (IoT RA) CD Stage' (2016) <www.iso.org> accessed 22 September 2021.

[30] Rayes and Salam (n 13) 67–69.

[31] National Research Council, *Expanding the Vision of Sensor Materials* (National Academies Press 1995) 10.

[32] EU directive 2004/108/EC (previously 89/336/EEC) on EMC defines the rules for the distribution of electric devices within the European Union.

[33] Sonia Ben Dhia, Mohamed Ramdani and Etienne Sicard, *Electromagnetic Compatibility of Integrated Circuits* (Springer US 2006).

or person over a short time interval[34]. This data collection process involves a phenomenon called transduction: sensing technologies convert signals gathered from the physical world into electrical signals. Any kind of physical input, such as motion, sound, pressure, or temperature, can be sampled, encoded, and represented in binary code for transmission over a network[35]. Once data is captured, actuators are in charge of controlling or taking action in IoT systems by converting sensor-collected data to motion[36]. In other words, they "acts" on the physical world, "converting an electrical form into tangible manipulation of the physical world"[37].

Device-wise, IoT will encompass a wide array of *things*, which span from fully capable peripherals to highly constrained devices. The latter typically have limited energy resources to spend on processing and communication[38]: this would therefore affect the other two layers. The third section of this chapter will specifically address resource-constrained device scenarios.

1.1.2 Network layer

Without dwelling too extensively on the complex architecture of the IoT network layer, which would exceed the scope of this study, an overview of IoT network models and protocols is nonetheless in order. A preliminary consideration should acknowledge that data are shared in IoT networks continuously: "from sensors to gateways and from gateways to data centres in enterprises, or from sensors to gateways for residential services such as video from home monitoring systems to the homeowner's smartphone while he's in a coffee shop"[39].

As these data are prone to a number of attacks (e.g., man in the middle, spoofing, sniffing etc.), it follows that network security is of paramount importance in IoT security (section 1.4.2). This layer illustrates how IoT components *communicate* within the Internet infrastructure. Therefore, it necessarily involves the OSI model and the TCP/IP protocol[40], which provides for end-to-end connectivity detailing the procedure for packetising, addressing, transmitting, routing and receiving data at the destination[41]. Notably, the ITU does not necessarily consider IP as a *constituent* part of the

---

[34] Rayes and Salam (n 13) 76–80.

[35] Denardis (n 17) 46–47.

[36] Rayes and Salam (n 13) 82.

[37] Denardis (n 17) 46.

[38] A Bormann, C., Ersue, M., & Keranen, 'RFC 7228: Terminology for Constrained-Node Networks', vol 39 (2014) 3 <http://dx.doi.org/10.1016/j.biochi.2015.03.025%0Ahttp://dx.doi.org/10.1038/nature10402%0Ahttp://dx.doi.org/10.1038/nature21059%0Ahttp://journal.stainkudus.ac.id/index.php/equilibrium/article/view/1268/1127%0Ahttp://dx.doi.org/10.1038/nrmicro2577%0Ahttp://> accessed 31 January 2020.

[39] Rayes and Salam (n 13) 7.

[40] Whereas IPv4 could provide for 4.3 billion addresses, IPv6 has room for 2^{128} or 340 trillion trillion trillion addresses.

[41] Mohammed M Alani, *Guide to OSI and TCP/IP Models* (Springer International Publishing 2014) <http://link.springer.com/10.1007/978-3-319-05152-9> accessed 20 September 2021.

IoT since its network infrastructure might be realised through "evolving networks, such as next generation networks (NGN)"[42].

Rayes and Salam argue that the IoT Network layer can be classified into three main characteristics: end-to-end delay, as the amount of time (typically in fractions of seconds) for a packet to travel across the network from source to destination; packet loss, occurring when at least one packet of data travelling across a network fails to reach its destination; network throughput, as the maximum amount of data moved successfully between two end points in a given amount of time[43].

For the sake of simplicity, IoT data transmission and processing scenarios are plotted in this network layer section in a scalable fashion, according to the needs of mostly IoT resource-constrained devices. Data might firstly be processed *at the edge* (edge computing): in other words, close to the devices who collected them. Data will then be transmitted to the "fog layer" (fog computing) and finally to the more widely known cloud computing.

The first technology under scrutiny is edge computing, which follows a distributed paradigm: information processing is located close to the edge, so to speak, where things and people produce or consume that information[44]. It is worth noting that it does not involve a small data centre or a small standalone device computing: it still resolves to cloud resources. Nevertheless, from a data protection perspective, the "edge paradigm" may reduce several security risks, as data would be encrypted locally – if lightweight protocols are in place, as shown by section 1.3 – "and translated into a secure communication protocol before being sent to the data center or storage resources shared in the cloud"[45].

Fog computing, albeit conceptually different from edge computing, is similar to edge and cloud technologies[46] for it is defined by NIST as a "layered model for enabling ubiquitous access to a shared continuum of scalable computing resources; [it] facilitates the deployment of distributed, latency-aware applications and services, and consists of fog nodes (physical or virtual), residing between

[42] ITU-T (n 26) 4.

[43] Rayes and Salam (n 13) 48–51.

[44] Rob van der Meulen, 'What Edge Computing Means For Infrastructure And Operations Leaders' (2018) <https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders> accessed 20 September 2021.

[45] Dianora Poletti, 'IoT and Privacy' in Roberto Senigaglia, Claudia Irti and Alessandro Bernes (eds), *Privacy and Data Protection in Software Services* (Springer 2022) 180.

[46] Shanhe Yi, Cheng Li and Qun Li, 'A Survey of Fog Computing: Concepts, Applications and Issues' (2015) 2015-June Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) 37, 37–42.

smart end-devices and centralised (cloud) services"[47]. All in all, fog computing is a computing architecture that uses devices – which can be independent components or could be built on top of existing gateways – to carry out a significant part of computation (usually, pre-processing), storage and communication before forwarding data to the cloud domain. The rapid data sharing of IoT highlighted the necessity of augmenting and spreading the cloud infrastructure with processing and storage functions that move with the "things". Fog computing, therefore, is a layer of computation between the device and the cloud: "[c]loud computing is brought closer to the data sources, the Things[:] *Cloud* becomes *Fog* when it is closer to *Things*, pun intended. […] Fog augments the Cloud to achieve the required pervasiveness and reliability required by rapid mobility in IoT"[48].

Albeit fog and cloud domains bear striking similarities – starting from the fact that they are both virtualised environments, they do differ in terms of location, mobility and computing capacity. Firstly, fog devices are located in proximity to the smart objects (unlike the "far" cloud servers), resulting in quicker responses; secondly, as the location of the smart things changes, the respective fog domain's virtual machines must be located on the closest fog devices; thirdly, fog devices have a lower computing power than cloud servers[49].

1.1.3 Application platform layer

On a preliminary note, the distinction between the application layer of the TCP/IP model and the IoT application level is substantial and crucial: whilst the former pertains to the IoT Network level, the latter aims at assuring abstraction across the numerous devices and sources of data. In other words, its function is to integrate all enabling technologies and constituting components – transcending vertical solutions – into a common, open, and multi-application environment. It allows for the management and control of a range of systems and processes: "the operation of this platform requires a comprehensive and diverse set of requisites to gather relevant data, analyse it, and create actionable insights"[50].

As shown by Rayes and Salam, the key features of this level boil down to 4 macro areas: i) traditional management (e.g., configuring, deploying, performance monitoring, security management); ii) application management (e.g., software/firmware installation, parching, debugging); iii) application development (e.g., data management, temporary caching, permanent storage); iv) application services

[47] Michaela Iorga and others, 'Fog Computing Conceptual Model' (2018) 2 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf> accessed 20 September 2021.

[48] Rayes and Salam (n 13) 157.

[49] ibid 225.

[50] ibid 181.

(e.g., data analytics, subscriptions and notification)[51]. Therefore, the "application level" is responsible for monitoring and controlling IoT elements in IoT's device, network and processing layers.

From a (EU) data protection perspective (covered by Chapter four), the above reflects one part of the conundrum raised by IoT data sharing and processing, that being the difficult of allocating accountability, and therefore responsibility and liability, to the multifold parties along IoT supply chain – device and integrated device manufacturers, application developers, software development houses, social platforms, further data recipients, data platforms, and standardisation bodies[52] – in terms of (personal) data processing.

1.2 IoT Domains

The cloud domain holds the IoT applications that are performing different operations on the data collected by the IoT objects[53]. Since the aim of this thesis is to study baseline IoT security and privacy aspects in a horizontal and cross-sectorial fashion, this section will not dwell too extensively on the diverse technical requirements and legal challenges of the different verticals – with the exception of the impact of security threats being determined by the criticality of the different assets, depending on the different use case scenarios. EU IoT Large-Scale Pilot Programme presents the most significant application domains for the Single Market, each of which has been covered by one or more projects, since IoT infrastructure has already been implemented in several sectors, both private and public: from healthcare (eHealth) to industrial processes (industry 4.0 – which stands for the fourth industrial revolution[54]), domestic appliances (smart homes), pervasive interconnectedness in the urban sphere (smart cities), agriculture (smart farming) and automotive (smart vehicles).

1.2.1 eHealth

Healthcare is arguably the most crucial vertical in IoT, as the promise here is to enhance and improve the effectiveness and efficiency of health care, therapies and, more generally, of monitoring people's vital states. Devices in combination with mobile apps allow patients to capture their health data easily and send medical information for up-to-the-minute analysis, as exemplified by the "smart pill"

[51] ibid 182.

[52] Poletti (n 45) 177.

[53] Rayes and Salam (n 13) 216.

[54] Klaus Schwab, 'The Fourth Industrial Revolution: What It Means and How to Respond | World Economic Forum' (2016) <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> accessed 28 September 2021: the fourth industrial revolution is characterised by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.

approved by the U.S. FDA with a "digital ingestion tracking system"[55]. Besides the abovementioned opportunities, the digitalisation of healthcare also raises normative questions pertaining to the ethical, social and legal fields. These are: the implications of subjectivities and embodiment in the world of eHealth; the political dimensions and power relations underlying the deployment of these technologies; the protection of individual and collective privacy and data protection fundamental rights[56]. Especially in the healthcare sector, (cyber)security and safety are closely intertwined, as the former affects the latter on an unprecedented scale. To cite the most notorious case only, technical research demonstrated how pacemakers could be hacked, exposing patients' safety and privacy[57].

Against this background, *ACTIVAGE* is a European IoT Large-Scale Pilot funded by the European Union's Horizon 2020 research and innovation programme. It aims at enabling Active & Healthy Ageing IoT based solutions and services, supporting and extending the independent living of older adults in their living environments, and responding to the real needs of caregivers, service providers and public authorities[58].

1.2.2 Smart farming

The UN's Food and Agriculture Organization (FAO) estimated that the current world population of 7.3 billion is expected to reach 9.7 billion in 2050[59]. As a consequence, the world will need to produce 70% more food in 2050 than it did in 2006 in order to feed the Earth's growing population[60]. IoT is well suited to transform the agriculture industry by enabling and empowering farmers to increase the quantity and quality of their crops at reasonable costs. Of the IoT sensor-based agriculture solutions it is worth mentioning advanced yield monitoring, optimal seeding, optimal water usage, livestock monitoring, and farming as a service[61]. Against the backdrop of connectivity limitation in remote areas, a major issue to be overcome at the IoT network layer, long-range communication technologies for IoT, such as IEEE 802.11 and LoRa/LoRaWAN, are the most reliable since cellular networks and

[55] FDA, 'FDA Approves Pill with Sensor That Digitally Tracks If Patients Have Ingested Their Medication ' (2017) <https://www.fda.gov/news-events/press-announcements/fda-approves-pill-sensor-digitally-tracks-if-patients-have-ingested-their-medication> accessed 28 September 2021.

[56] Deborah Lupton, 'M-Health and Health Promotion: The Digital Cyborg and Surveillance Society' (2012) 10 Social Theory & Health 2012 10:3 229 <https://link.springer.com/article/10.1057/sth.2012.6> accessed 21 September 2021.

[57] Daniel Halperin and others, 'Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses', *2008 IEEE Symposium on Security and Privacy* (IEEE 2008); Aakarsh Rao and others, 'Probabilistic Threat Detection for Risk Management in Cyber-Physical Medical Systems' (2017) 35 IEEE Software 38.

[58] See https://www.activageproject.eu/activage-project/#About-ACTIVAGE

[59] https://www.un.org/en/development/desa/news/population/2015-report.html

[60] See <http://www.fao.org/e-agriculture/news/why-iot-big-data-smart-farming-are-future-agriculture> accessed March 2021.

[61] Rayes and Salam (n 13) 242.

5G technologies would hardly fit into the agricultural context due to availability and economic feasibility issues[62].

The *IOF2020* IoT Large-Scale Pilot project seeks to automatise most of the field operations through the adoption of IoT autonomous objects. Of course, farmers would still be in charge of the processes: nevertheless, the focus of their activity would be on market choices and taking care of communications with customers. After execution of the field work, the measured data are automatically returned from the machine to the office through the cloud. This is the basis for subsequent tasks. Moreover, such data are also provided to research institutes, which feed them into computer models for further improvement[63].

1.2.3 Smart homes

Smart Home is an emerging application paradigm which has been gaining increasing popularity. Most recently, the Internet of Things (IoT) has been fostering a vision of domotics, where users can install connectable devices and appliances in their domestic network to automatically and synergically manage home services and functionalities. This emerging market is rapidly encouraging software manufacturers and developers to produce novel applications, services and products, to provide additional smart home functionalities. In this regard, an EU Commission JRC technical report provides an overview of state-of-the-art smart home technical standards, protocols and technologies deployed (e.g., sensors, networks, etc.)[64]. Notwithstanding, noticeable legal concerns still exist. They are mainly related to cybersecurity, safety and privacy, as well as to the protection of collected, shared and processed personal data, most of which could be sensitive pursuant to the EU General Data Protection Regulation (GDPR)[65].

SIFIS-Home is a European project funded by Horizon 2020 that aims to provide a secure-by-design and consistent software framework for improving resilience of Interconnected Smart Home Systems at all stack levels. To this end, the framework enables the development of security, privacy aware and accountable applications, algorithms and services, and makes it possible to detect and dynamically

[62] Nahina Islam and others, 'A Review of Applications and Communication Technologies for Internet of Things (IoT) and Unmanned Aerial Vehicle (UAV) Based Sustainable Smart Farming' (2021) 13 Sustainability 1821, 5–6 <https://www.mdpi.com/2071-1050/13/4/1821/htm> accessed 21 September 2021.

[63] See <https://www.iof2020.eu/> accessed March 2021.

[64] P Bertoldi and T Serrenho, 'Smart Home and Appliances: State of the Art - Energy, Communications, Protocols, Standards' (2019) Publications Office of the European Union.

[65] Olga Gkotsopoulou and others, 'Data Protection by Design for Cybersecurity Systems in a Smart Home Environment' [2019] Proceedings of the 2019 IEEE Conference on Network Softwarization: Unleashing the Power of Network Softwarization, NetSoft 2019 101.

react to cyber-attacks and intrusion attempts or violation of user-defined policies, thus increasing control and trust of Smart Home end users[66].

1.2.4 Smart cities

A smart city is a place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and business. A smart city goes beyond the use of information and communication technologies (ICT) for better resource use and fewer emissions. It means smarter urban transport networks, upgraded water supply and waste disposal facilities, and more efficient ways to light and heat buildings. It also means a more interactive and responsive city administration, safer public spaces and meeting the needs of an ageing population[67]. Whereas technical literature focuses on smart city rankings, in terms of techno-assets[68], technical standards[69] and enabling technologies[70], legal scholars elaborate on different governance approaches to the smart city. Neoliberal approaches have been criticised due to their intrinsic commodification, or *datafication*, of citizens who tend to assume a passive role "with companies and city administrations performing forms of civic paternalism (deciding what's best for citizens) and stewardship (delivering on behalf of citizens)"[71].

Against this background, the *SynchroniCity* European IoT Large-Scale Pilot aims to open up a global market for IoT-enabled services for cities and communities, where public authorities and businesses develop and deploy services using new technologies in agile partnerships to sustain and improve the lives of citizens, and to ensure sustainable local economic development[72]. The special attention devoted by the EU to tackling smart cities issues is reflected in a second European IoT Large-Scale Pilot, namely *MONICA*. It involves six major cities in Europe: Lyon, Bonn, Leeds, Turin, Copenhagen and Hamburg. Several applications are deployed,

---

[66] See <https://www.sifis-home.eu/> accessed March 2021.

[67] See <https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en#:~:text=The%20Smart%20Cities%20Marketplace%20is,%2C%20banks%2C%20research%20and%20others.&text=It%20builds%20on%20the%20engagement,and%20participate%20in%20city%20governance> accessed March 2021.

[68] Rudolf Giffinger and others, 'Smart Cities-Ranking of European Medium-Sized Cities' (2007) <http://www.smart-cities.eu> accessed 22 September 2021.

[69] Chun Sing Lai and others, 'A Review of Technical Standards for Smart Cities' (2020) 2 Clean Technologies 290.

[70] Zaib Ullah and others, 'Applications of Artificial Intelligence and Machine Learning in Smart Cities' (2020) 154 Computer Communications 313.

[71] Paolo Cardullo and Rob Kitchin, 'Smart Urbanism and Smart Citizenship: The Neoliberal Logic of "citizen-Focused" Smart Cities in Europe' (2019) 37 Politics and Space 813, 814.

[72] See <https://synchronicity-iot.eu/synchronicity-rolls-out-49-answers-to-successfully-scaling-iot-solutions-for-smart-cities-and-communities/> accessed February 2021.

using IoT-enabled devices such as smart wristbands, video cameras, loudspeakers and mobile phones It focuses on one of the key aspects of European society: cultural performances in open-air settings which create challenges in terms of crowd safety, security and noise pollution. MONICA will develop, deploy and demonstrate three IoT ecosystems on security, acoustics and innovation, addressing real user needs[73].

1.2.5 Smart vehicles

According to ENISA, *smart cars* can be defined by the integration of connected components in the car in order to bring added-value services to drivers and passengers. Strictly connected, *Intelligent Road Systems* can be defined by the integration of connected cyber-physical components along the road that allow road operators to monitor and optimise traffic conditions (e.g., traffic information panels). As these two domains rely on the Internet of Things and cyber physical-systems, cyber threats have real consequences on the safety of citizens[74].

AUTOPILOT is a European IoT Large-Scale Pilot funded by the European Union's Horizon 2020 research and innovation programme. The objectives are to increase safety, provide more comfort and create many new business opportunities for mobility services by developing new services on top of IoT involving autonomous driving vehicles, like autonomous car sharing, automated parking, or enhanced digital dynamic maps to allow fully autonomous driving. AUTOPILOT IoT enabled autonomous driving cars are tested, in real conditions, at four permanent large-scale pilot sites in Finland, France, Netherlands and Italy, whose test results will allow multi-criteria evaluations (technical, user, business, legal) of the IoT impact on pushing the level of autonomous driving[75].

1.3 The "Resource-Constrained" Paradigm

Historically, devices connected to the internet could have been grouped into a homogeneous class, that is, fully capable computers or peripherals with endless sources of power, embedding big and costly hardware. This classification is no longer true within the IoT network, which combines devices with limited CPU, memory and processing power e.g., pressure sensors, and devices with powerful processors, large memory and replenishable sources for energy e.g., smartphones. In fact, recalling Marwedel, a comprehensive overview of the huge class of embedded systems' hardware

[73] See <https://www.monica-project.eu/home/about-monica/> accessed February 2021.

[74] See <https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-transport> accessed February 2021.

[75] See https://european-iot-pilots.eu/project/autopilot/

components[76] could hardly be drawn since they are far less standardised than hardware for personal computers[77]. The exhibition of significant differences in available execution environments, processing, and storage capabilities would add an extra layer of difficulty. In other words, a structured approach is needed in order to uniformly and transparently deploy application components onto a large number of heterogeneous devices[78].

An IETF report listed the prominent facets to the constraints on nodes, or devices, often applied in combination. They are constraints on the maximum code complexity (ROM/Flash); constraints on the size of state and buffers (RAM); constraints on the amount of computation feasible in a period of time ("processing power"); constraints on the available power; and constraints on the user interface and accessibility in deployment (ability to set keys, update software, etc.)[79]. Whereas constraints in networks may include low achievable bitrate, high packet loss and high variability of packet loss (delivery rate)[80].

IETF RFC 7228 designed a taxonomy[81] of constrained devices based on two dimensions: processing power and memory. It recognises three classes of devices accordingly:

> *Class 0 devices are very constrained sensor-like motes. They are so severely constrained in memory and processing capabilities that most likely they will not have the resources required to communicate directly with the Internet in a secure manner (rare heroic, narrowly targeted implementation efforts notwithstanding). Class 0 devices will participate in Internet communications with the help of larger devices acting as proxies, gateways, or servers.*
>
> *Class 1 devices are quite constrained in code space and processing capabilities, such that they cannot easily talk to other*

[76] Peter Marwedel, *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things* (2018) Springer, 126.

[77] Ugo Pagallo, Massimo Durante and Shara Monteleone, 'What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT', *Data protection and privacy: (in)visibilities and infrastructures* (Springer, Cham 2017) 74–75.

[78] Michael Vögler and others, 'LEONORE - Large-Scale Provisioning of Resource-Constrained IoT Deployments' (2015) 30 Proceedings - 9th IEEE International Symposium on Service-Oriented System Engineering, IEEE SOSE 2015 78, 78 <http://www.busybox.net> accessed 31 January 2020.

[79] A Bormann, C., Ersue, M., & Keranen, 'RFC 7228: Terminology for Constrained-Node Networks', vol 39 (2014) 5.

[80] ibid, 6.

[81] Even though they both belong to the classification methods process; taxonomies are substantially different from typologies. The former deals with abstract and theoretical framework, built upon "ideal types" (Weber, 1949), whilst the latter categorises constructive and empirical entities (Bailey, 1994). Since the analysis at stake deals with inner mechanisms and components, it seems natural to adopt a taxonomical approach to the problem.

> *Internet nodes employing a full protocol stack such as using HTTP, Transport Layer Security (TLS), and related security protocols and XML-based data representations. However, they are capable enough to use a protocol stack specifically designed for constrained nodes (such as the Constrained Application Protocol (CoAP) over UDP [COAP]) and participate in meaningful conversations without the help of a gateway node. In particular, they can provide support for the security functions required on a large network.*
>
> *Class 2 devices are less constrained and fundamentally capable of supporting most of the same protocol stacks as used on notebooks or servers. However, even these devices can benefit from lightweight and energy-efficient protocols and from consuming less bandwidth. Furthermore, using fewer resources for networking leaves more resources available to applications*[82].

The involvement of sensors with limited energy and storage inevitably brings several security and privacy considerations in terms of authentication, mobility, wirelessness, embedded use, diversity, and scale. Without dwelling on these issues too extensively at this point, as they are addressed in the following chapters, it is worth bringing forth one major consequence of these constraints regarding network security.

Computational power[83] in IoT systems can be plotted in a scalable fashion, from cloud services to resource-constrained nodes. "Much of the computational power used to aggregate, process and provide data to external utilities, such as other services or humans, resides in the core of the network in the form of cloud platforms. Towards the edge of the network, computational power drops off as we shift from intermediate aggregators, such as smart phones or local base stations, to low powered sensors with restricted memory"[84]. Constrained devices always resort to the cloud – or gateways, fog devices, etc. – for outsourced storage and computation[85]. Nevertheless, they may not have the necessary computational power to embed security software or to implement appropriate technical and

[82] Bormann, C., Ersue, M., & Keranen (n 38) 8–9.

[83] Massimo Durante, *Computational Power: The Impact of ICT on Law, Society and Knowledge* (Routledge 2021).

[84] Robert Hegarty and John Haggerty, 'Presence Metadata in the Internet of Things: Challenges and Opportunities', *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)* (2020) 632.

[85] Jun Zhou and others, 'Security and Privacy for Cloud-Based IoT: Challenges' (2017) 55 IEEE Communications Magazine 26, 26–33.

organisational measures such as encryption, authentication and pseudonymisation[86] in order to secure communication channels. In particular, encryption is the cornerstone of network security protocols. A study by HP Fortify reported that 70% of the devices do not encrypt communications to the Internet and local network, while half of the devices' mobile applications performed unencrypted communications to the cloud, Internet or local network[87]. Cheruvu et al. suppose that in a constrained scenario, the percentage of security-related computing might be more than half of the overall device's resources, whilst it typically stands at around 15% of the total resources' cost[88].

The need to secure data transfer in IoT networks led to investing particular efforts in setting up lightweight[89] protocols suited to the needs of constrained nodes/devices. A successful application protocol for IoT devices, since it can be used on top of the IPv6 infrastructure[90] through the 6LoWPAN protocol (which enables IPv6 in resource-constrained scenarios), is the Constrained Application Protocol (CoAP), which can be coupled with Datagram Transport Layer Security (DTLS) to encrypt and authenticate messages[91]. Against the background of lightweight encryption, where there is a trade-off between performance and security, in 2015 US NIST started a project to and standardise lightweight cryptographic algorithms that are suitable for use in constrained environments, where the performance of current NIST cryptographic standards is not acceptable[92]. In March 2021, NIST announced the ten finalists that made it through to the second round[93].

According to some authors, a decisive cause for such constrained hardware is purely economic: "to allow mass deployment of IoT devices, businesses want the cost per unit to be as inexpensive as possible"[94]. Moreover, the limited size and computational power can be affected by other reasons, such as environmental (e.g., meteorological sensors in remote and hard-weather condition areas) or

---

[86] European Union Agency for Fundamental Rights, *Manuale sul diritto europeo in materia di protezione dei dati* (EU publishing office, Luxembourg 2018).

[87] Hewlett Packard, 'HP News - HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack' (2014) <https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676>.

[88] Sunil Cheruvu and others, *Demystifying Internet of Things Security* (2020) APRESS Open 11.

[89] It means that the algorithm under scrutiny has a small-implementation code.

[90] Anuj Sehgal and others, 'Management of Resource Constrained Devices in the Internet of Things' (2012) 50 IEEE Communications Magazine 144.

[91] Philippe Pittoli, Pierre David and Thomas Noël, 'Security Architectures in Constrained Environments: A Survey' (2018) 79 Ad Hoc Networks 112, 121 <https://doi.org/10.1016/j.adhoc.2018.06.001>.

[92] NIST, 'Lightweight Cryptography | CSRC' <https://csrc.nist.gov/Projects/lightweight-cryptography> accessed 20 September 2021.

[93] For a technical assessment of the ten NIST's finalists, see Fabio Campos and others, 'Assembly or Optimized C for Lightweight Cryptography on RISC-V?' (2020) 12579 LNCS Lecture Notes in Computer Science 526 <https://link.springer.com/chapter/10.1007/978-3-030-65411-5_26> accessed 20 September 2021.

[94] Farhan Siddiqui and others, 'Secure and Lightweight Communication in Heterogeneous IoT Environments' (2021) 14 Internet of Things <https://doi.org/10.1016/j.iot.2019.100093> accessed September 2021, 2.

contextual to the system in which they are embedded[95]. In other words, to scale up the spread of affordable and physically feasible Internet technologies, the characteristics of the nodes on which (IoT) networks are built need to be scaled down.

A promising answer to the above-mentioned problems may come from research into chips' architecture. Research published in August 2022 in Nature presented NeuRRAM, a resistive random-access memory (RRAM)-based chip for supporting AI applications on edge devices[96]. "Currently, AI computing is both power hungry and computationally expensive. Most AI applications on edge devices involve moving data from the devices to the cloud, where the AI processes and analyses it. […] By reducing power consumption needed for AI inference at the edge, this NeuRRAM chip could lead to more robust, smarter and accessible edge devices and smarter manufacturing. It could also lead to better data privacy as the transfer of data from devices to the cloud comes with increased security risks"[97]. In this respect, the announcement of an EU Chips Act[98] will be central to the creation of a European chip ecosystem. This will include production, as well as connecting the EU's world-class research, design and testing capacities[99].

While awaiting a full-scale deployment of technical solutions such as lightweight encryption or NeuRRAM-like chips, the present is made up of IoT systems with constrained hardware. Even though it may sound trivial, while many devices connecting to the IoT are constrained, the networks connecting them will also be constrained[100]. Therefore, from a methodological viewpoint, this study relies on the assumption that IoT systems always involve constrained technologies, which are typically sensors at the device layer – following IoT architecture taxonomy in section 1.1 – regardless of potentially unconstrained technologies connected to these systems. Every layer of the taxonomy presented in section 1.1 has its own security vulnerabilities and threats. The next section aims to provide a general overview of the main security threats for the IoT.

---

[95] Timothy Stapko, *Practical Embedded Security: Building Secure Resource-Constrained Systems* (Newnes 2008) 85.

[96] Weier Wan and others, 'A Compute-in-Memory Chip Based on Resistive Random-Access Memory' (2022) 608 Nature 504.

[97] Ioana Patringenaru, 'A New Neuromorphic Chip for AI on the Edge, at a Small Fraction of the Energy and Size' (*UC San Diego News Center*, 17 August 2022) <https://ucsdnews.ucsd.edu/pressrelease/Nature_bioengineering_2022> accessed 29 August 2022.

[98] European Commission, 'State of the Union 2021 - Letter of Intent' (2021) 4 <https://ec.europa.eu/info/sites/default/files/state_of_the_union_2021_letter_of_intent_en.pdf>.

[99] See https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.

[100] Siddiqui and others (n 94) 3.

1.4 The IoT Security Threat Landscape

This section highlights the main security threats affecting IoT constrained and unconstrained devices. The goal is to capture the whole threats model. In other words, the issues related to back-end vulnerabilities: not only at device level, but also the web service connected to it. The so-called threat landscape has been classified in relation to the consequences the attack scenarios pose to the system (service compromising and sensing domain attacks), to enabling technologies (cloud and fog computing) or the underlying data sharing (packets crafting, packets alteration, traffic analysis). Thus, the horizontal nature of security applies to all the elements of the IoT taxonomy as in section 1.1.

The 2020 ENISA threat landscape – which combines 22 different reports by listing the major changes from the 2018 threat landscape – and the 2021 version – which focuses on 8 prime cyberthreat groups – have been used as a major source for modelling the knowledge of the attack vectors and consequences. Albeit the security threats under scrutiny are the same as "traditional" IT technologies, previous sections have shown that IoT complex architecture is to several extents different from conventional networks. Therefore, holistic mitigation techniques that take into account the vulnerabilities of all the IoT layers must be adopted to secure these open architectures[101].

ENISA, building on its threat taxonomy, tackled IoT security threats horizontally for the first time in 2017. The report groups IoT security threats under 7 macro-areas: i) nefarious activity/abuse (e.g., DDoS, malware, attacks on privacy, exploit kits, etc.); ii) eavesdropping/interception (e.g., man-in-the-middle, IoT communication protocol hijacking, network reconnaissance, etc.); iii) outages (e.g., devices/hardware failures, system failures, network outage, etc.); iv) damages/loss IT assets (e.g., data leakage); v) failures/malfunctions (e.g., third party failures, software vulnerabilities); vi) disasters (e.g., natural/environmental disasters); vii) physical attacks (e.g., device tampering, sabotage). According to the different application domain, security threats have different potential impacts. Therefore, the impact of each threat has been determined "by calculating a weighted average of the responses from the interviewees, which were based on a five-step scale that ranged from no importance to crucial importance"[102].

ENISA's sevenfold taxonomy has its virtues. It provides a systematic and comprehensive overview of the threats that can affect all the relevant assets in a IoT ecosystem: IoT devices, other IoT

[101] Syed Rizvi and others, 'Securing the Internet of Things (IoT): A Security Taxonomy for IoT' (2018) Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, 164.

[102] ENISA, 'Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures' (n 1) 33.

ecosystem devices, platform & backend, applications and services and finally network infrastructure and the information collected and shared *via* communication channels.

Yet, for the purposes of this work, it could be questioned whether the type-threat *attacks on privacy* can be subsumed under the first cluster i.e., nefarious activity/abuse. "Attacks on privacy" is generically described as a threat affecting "both the privacy of the user and the exposure of network elements to unauthorised personnel"[103]. Within the same category, ENISA lists malware, DDOS attacks, modification of information, targeted attacks, counterfeit by malicious devices and exploit kits. Chapter 2 will argue that cyber and information security requirements would be the "infrastructure", so to speak, of technical norms, controls and rules that are there to facilitate (or hinder, if not well implemented) the right to privacy and data protection. The GDPR defines a 'personal data breach' as "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"[104]. Therefore, it can be argued that threats to fundamental rights e.g., privacy and data protection, can result from the combination of, and, as a consequence of, *every* macro-area of the ENISA cybersecurity threat landscape.

Against this backdrop, *attacks on privacy*, if we were to use ENISA's classification, would pertain to a different level of abstraction and it should not be placed within the macro-category *nefarious activity/abuse.* For this reason, the model that follows only takes into consideration the threats posed to systems' cybersecurity, whereas privacy and data protection will be addressed later in Chapter 4.

[103] ENISA, 'Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures' (2017) 34.

[104] Regulation (EU) 2016/679, art. 4(12).

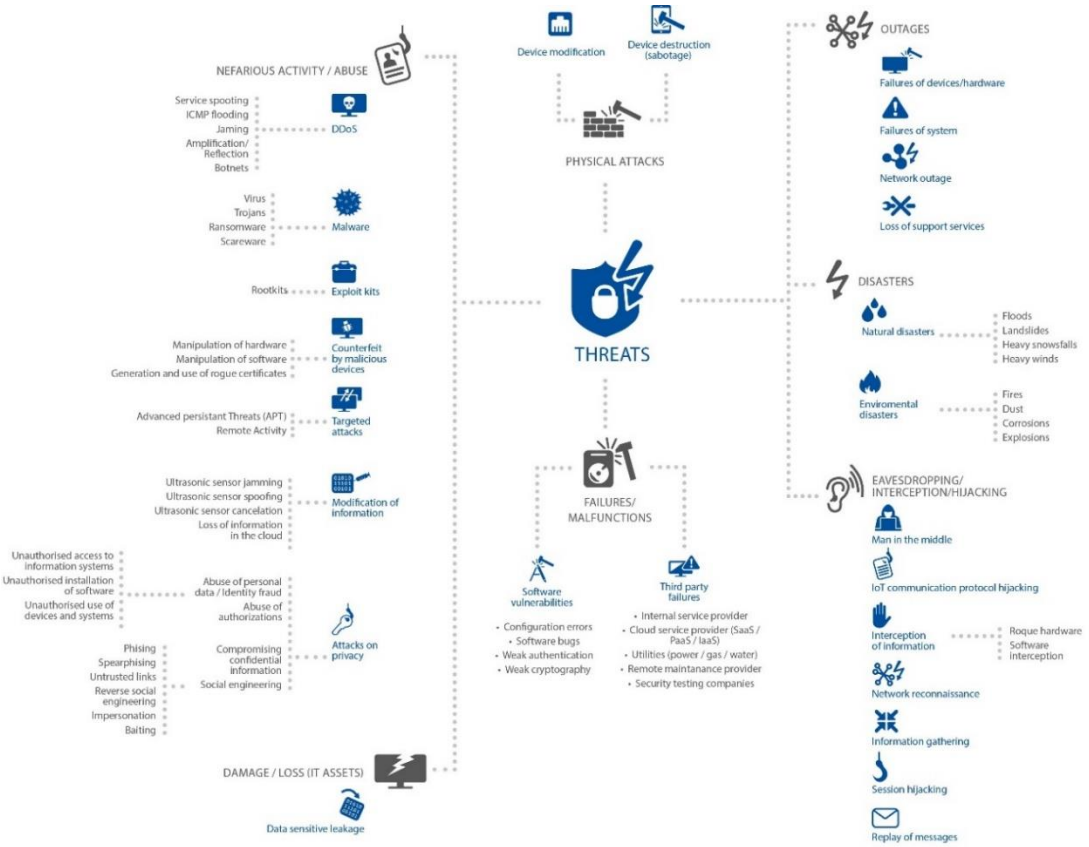


Figure 1: ENISA IoT Threats Taxonomy[105]

1.4.1 Device layer attacks

Sensor nodes usually use ad hoc network technology to dynamically change the network topology, allowing communication with the outer world. Sensed data is sent to fog devices; albeit a direct connection with fog devices – through wires – is possible, sensor nodes often use wireless communication due to the diversity of the deployment environment. In this scenario, attackers can easily eavesdrop on communication between these nodes. Furthermore, the attacker can directly access the related attributes of the device through physical attacks, and then start a further attack, such as tag cloning and spoofing attacks. For example, RFID technology is widely used in this layer: attackers can destroy communication between the reader and RFID tag, e.g., through RF jamming. In general terms, the attack of the perception layer usually aims at destroying the data collection and communication[106]. This section presents four types of attacks that may occur at either IoT device or

[105] ENISA, 'Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures' (n 1) 32.

[106] Kejun Chen and others, 'Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice' (2018) 2 Journal of Hardware and Systems Security 97 <https://doi.org/10.1007/s41635-017-0029-7> accessed 17 September 2021.

network architecture layer, following the taxonomy of section 1.1: jamming, vampire, select-forwarding, sinkhole.

The *jamming* attack causes a disruption in the service by interfering with the legitimate signals exchanged in the connection between the smart objects and the fog device. Because of interference at the connection level, from a classificatory standpoint, it can be also considered as a network layer attack. It can mainly take on two forms: receiver jamming or sender jamming. The former degrades the quality of the received signal: "as a result, the receiving end does not acknowledge the reception of these damaged packets and waits for the sender to retransmit those packets"[107]. The latter "prevents the neighbouring objects from transmitting their packets as they sense the wireless channel to be busy and back off waiting for the channel to become idle"[108]. Jamming attacks can also be classified according to the different strategies that a malicious agent may follow to attack. The best known being constant, deceptive, reactive and random jamming.

The *vampire* attack takes advantage of the fact that the environment of the device/physical/perception layer is generally restricted in terms of resource and power, as seen in section 1.3. Therefore, the resource-constrained devices use "sleep" to prolong life. A malicious agent could misbehave to force IoT resource-constrained nodes to consume extra amounts of power so that they run out of battery earlier[109]. In other words, attackers can keep the node in working state, by preventing it from switching to sleep, to accelerate the consumption of energy. This particular attack is also known as *denial of sleep*. Other vampire attacks differ to the extent that they use different strategies to drain power e.g., flooding attack, carrousel and stretch attacks[110].

The *selective-forwarding* attack occurs when the device cannot send its generated data packets directly to the fog layer but has to rely on other devices that lie along the path toward the fog device to deliver those packets. Against this background, the malicious device would not forward a part of the packets received[111]. In a constrained scenario, this attack is likely to be successful if mitigation solutions are not deployed: path redundancy is one of those, where packets are forwarded to neighbouring devices multiple times in order to get to the fog device.

The *sinkhole* attack, in a similar fashion to the *selective-forwarding* attack, operates through a malicious device claiming to have the shortest path to the fog device. In so doing, it attracts all

[107] Rayes and Salam (n 13) 228.

[108] ibid.

[109] ibid 230.

[110] ibid 230–231.

[111] ibid 232.

neighbouring devices that do not have the transmission capacity to reach the fog layer. Hence, they forward their packets to that malicious actor and count on that device to deliver their data. As a result, all the communication that stems from the neighbouring nodes flows through this malicious node. Needless to say, if the data packets are not encrypted, the malicious node has the ability to look at the content of all the forwarded packets[112].

1.4.2 Network layer attacks: a focus on fog and cloud domain

Attention, here, is devoted to the attacks that typically characterise the network level, such as data interception, packets alteration, etc. There are many kinds of networks in the IoT, the Internet is just one of them. Different networks use different protocols and are run by different devices, so the attacks on the network also vary. The most common IT attack is the Denial of Service (DoS) attack which can exhaust network resources and affect the availability of network service. Other than that, this section delves into traditional IT network attacks that can specifically affect IoT devices, such as distributed denial of service (DDoS), man-in-the-middle, replay, sniffing/eavesdropping and key logger.

Distributed Denial of Service (DDoS) attacks perhaps have become the best known and feared threat in the IoT domain, as the magnitude of the impact it could attain is unforeseeable. Several existing research works have investigated these increasing threats[113]. When such an attack is successful, users of a system or service are not able to access the relevant information, services or other resources. This stage can be accomplished by exhausting the service or overloading the component of the network infrastructure by access requests. Malicious actors increased the number of attacks by targeting more sectors with different motives. While defence mechanisms and strategies are becoming more robust, malicious actors are also advancing their technical skills[114]. In particular, IoT's vulnerability to such cyberattacks shall be observed from a twofold standpoint. On the one hand, 5G connectivity supports localised DDoS, "where an attacker interferes with the connectivity of a specific area covered by a slice through a set of compromised devices"; on the other, as addressed in the previous section, resource-constrained devices often lack necessary security techniques and controls to counter these threats[115].

---

[112] ibid 233.

[113] Emanuele Cozzi and others, 'Understanding Linux Malware' [2018] Proceedings - IEEE Symposium on Security and Privacy 161; Manos Antonakakis and others, 'Understanding the Mirai Botnet', *26th USENIX Security Symposium* (2017); Yin Minn Pa Pa and others, 'IoTPOT: Analysing the Rise of IoT Compromises', *WOOT '15* (2015).

[114] ENISA, 'ENISA Threat Landscape - Distributed Denial of Service' (2020) 2.

[115] ENISA, 'ENISA Threat Landscape 2021: April 2020 to Mid-July 2021' (2021) 69 <https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020>.

The *Man-in-the-Middle (MitM)* attack requires the attacker to place himself between two communicating parties and secretly forward messages for them, while the two original parties trust they are communicating securely and without any intermediation. The malicious actor can then monitor and eventually modify the information content. Albeit similar attacking patterns have always existed in the physical dimension long before digitisation, IoT data sharing brought MitM to a whole new level[116].

A *Replay* attack takes place when a malicious actor eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network, as the attack could be successful simply by resending the whole thing[117].

Sniffing is a popular attack used by malicious parties to capture and analyse network communication information. With sniffing, a malicious actor is able to eavesdrop data from network layers and, as a consequence, to link and steal valuable information[118].

Lastly, *Key logger* is a piece of hardware or a software programme that captures everything a user types on the keyboard[119].

Since the IoT taxonomy (section 1.1) presented fog and cloud computing within the network layer, it seems appropriate to emphasise here that cloud and fog domain attacks are particularly relevant to the IoT field. Nevertheless, the discussion will not dwell on them too extensively given their high degree of technicality. Rayes and Salam summarise the most common security attacks in the cloud domain. The *hidden-channel attack* exploits shared hardware components, such as the cache, among the Virtual Machines (VMs) running on the same server: as a result, data could be leaked across VMs that are hosted by the same server[120]. The *VM migration attack* exploits VM migrations from one server to another, which is useful *per se* when a server needs to go offline for maintenance or for patch installation. The malicious agent either attacks the module which is responsible for managing the migration process by exploiting a bug in the software or attacks the network links over which the VM is moved (*via* a sniffing or a man-in-the-middle attack)[121]. The *theft-of-service attack* materialises

[116] See https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/man-in-the-middle

[117] See https://www.kaspersky.com/resource-center/definitions/replay-attack

[118] ENISA, 'ENISA Threat Landscape for 5G Networks' (2019) 59.

[119] ENISA, 'Malicious Software - Train the Trainer Reference Guide' (2010) 17.

[120] Rayes and Salam (n 13) 217.

[121] ibid 220–221.

when a malicious VM deceives the hypervisor by getting assigned more resources than it is supposed to receive. The other VMs – the targets of the attack – then get allocated a smaller share of resources than they should actually obtain, which in turn degrades their performance[122]. The *VM escape attack* exploits, again, a software bug in the hypervisor in order to circumvent VM isolation, which prevents access to VMs data from other VMs hosted by the same server[123]. Finally, *insider attacks* consider the case when cloud data centre administrators unlawfully access and modify data[124].

Albeit fog and cloud share many similarities – as seen in section 1.1.4, there are several security threats specific to the fog domain. "Unlike cloud data centres which are offered by well-known companies, fog devices are expected to be owned by multiple and lesser-known entities"[125]: identity authentication of the fog device and trust are therefore crucial. Secondly, VMs migration, in the fog domain, takes place over the Internet rather than over cloud's internal network: the chance of being exposed to compromised nodes or routers is considerably higher. Finally, due to resource constraints, fog devices are more prone to Dos and DDoS than data centres[126].

1.4.3 Application layer attacks

The last layer of the IoT architecture i.e., application, has its own vulnerabilities and attack vectors. The attacks in the application layer mainly target data, possibly sensitive, of the users by seeking (unauthorised) access. This can be done by stealing credentials, by counterfeiting identity of legitimate users or by exploiting the vulnerabilities of programmes and application (e.g., code injection, buffer overflow). Social engineering[127] techniques are increasingly refined and effective: AI tools facilitate automated personalised attacks using information gathered online[128]. In addition to these attacks, the application layer is also threatened by so-called "viruses", malicious software like malware and Trojans. This section takes into account five attacks. They are: SQL injection, malware, ransomware, masquerading and zero-day.

---

[122] ibid 222.

[123] ibid 223.

[124] ibid 223–224.

[125] ibid 226.

[126] ibid.

[127] ENISA defines "social engineering" as all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons. See < https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering> accessed 21 September 2021.

[128] ENISA, 'Artificial Intelligence Threat Landscape Report ' (2020) <https://www.enisa.europa.eu/news/enisa-news/enisa-ai-threat-landscape-report-unveils-major-cybersecurity-challenges> accessed 21 September 2021.

SQL Injection (SQLi) aims to attack the databases that either store or deliver the required information to web services and applications. SQLi are the most common threats against such services, corresponding to two thirds of web application attacks[129].

Malware is perhaps the most famous cyberattack, which occurs in the form of malicious software. The genus malware includes the types crypto-miners, viruses, ransomware, worms and spyware. Its common objectives are information or identity theft, espionage and service disruption[130]. Although malware detections has globally remained at the same levels as in 2018, the ENISA 2020 report observed a 13% increase in malware targeting businesses in services, education and retail among the worst affected sectors[131]. Interestingly, 2020 represented a "never-seen-before spike in IoT malware" – as reported by ENISA in the 2021 threat landscape – mostly due to unpatched devices[132].

Ransomware is a type of malware that infects the computer systems of users and manipulates the infected system in such a way, usually by encrypting user's files, that the victim cannot (partially or fully) use it and the data stored on it. In such cases, the ransomware victim may suffer economic losses either by paying the ransom demanded or by paying the cost of recovering from the loss, if they do not comply with the attacker's demands. These attacks are one of the main reasons for the increased interest in this type of insurance over the last 5 years. At the time of writing, the most known (and critical) types of ransomwares are *Lockergoga*, *Katyusha*, *Jigsaw*, *Pewcrypt*, *Ryuk* and *Dharma*. Whereas the most targeted sectors are States, educational institutions, the health sector and cloud service providers[133]. Recent research shows a higher curve towards IoT ransomware "attacks which is expected to be 5 times higher by 2020 and it will exceed more than 6 trillion dollars as ransom against ransomware attacks [:] every 11 s a ransomware attack will occur around the globe"[134].

In the *masquerading* attacks, one entity illegitimately assumes the identity (e.g., a network identity) of another in order to benefit from it[135].

Finally, "*Zero-Day*" is cybersecurity jargon for the opportunity to exploit a software vulnerability that is not yet publicly known and, by extension, the vulnerability itself. Attacks against these

---

[129] ENISA, 'ENISA Threat Landscape 2020 - Web Application Attacks' (2020) 2 <https://www.enisa.europa.eu/publications/web-application-attacks> accessed 20 September 2021.

[130] ENISA, 'ENISA Threat Landscape 2020 - Malware' (2020) 2 <https://www.enisa.europa.eu/publications/malware> accessed 20 September 2021.

[131] ibid 7.

[132] ENISA, 'ENISA Threat Landscape 2021: April 2020 to Mid-July 2021' (n 115) 85.

[133] ENISA, 'ENISA Threat Landscape 2020 - Ransomware' (2020) 2–13 <https://www.enisa.europa.eu/publications/ransomware> accessed 20 September 2021.

[134] Mamoona Humayun and others, 'Internet of Things and Ransomware: Evolution, Mitigation and Prevention' (2021) 22 Egyptian Informatics Journal 105.

[135] ENISA, 'Reference Incident Classification Taxonomy Task Force Status and Way Forward' (2018) 10.

vulnerabilities are also called "Zero-Days" in the mainstream media [136]. To make things more complex, law enforcement and intelligence agencies, by exploiting zero-days vulnerabilities, can more easily install malware in computer systems for law enforcement purposes[137], at the price of exposing the users of the system in question to attacks by malicious actors[138]. Thus, vulnerability of software is a sensitive issue that intersects the conflicting interests of cybersecurity (and, together, of privacy and personal data protection) and national security, as testified by the recent "Pegasus" scandal[139].

1.4.4 The missing piece of the jigsaw: IoT supply chain security threats

The traditional concept of establishing a security perimeter i.e., identifying all the relevant assets to protect and setting up the essential equipment and technologies to prevent outside attacks, becomes an extremely complicated task with the advent of ubiquitous IoT. As shown in the previous section, the IoT architecture disproportionately amplifies the attack surface, and the compelling need to secure the supply chain across the IoT ecosystem would make the identification of a perimeter extremely challenging. In turn, organisations are increasingly at risk of being attacked and breached through one of their suppliers. "Organisations have many vendors, several of which in turn have multiple large corporate and government clients, therefore mapping this cyber-ecosystem of connections of surfaces will be very difficult, as it may involve these other organisations to divulge sensitive information regarding their relationships with other companies"[140].

Whereas US NIST defines the ICT supply chain as "the integrated set of components (hardware, software, and processes) within the organisational boundary that composes the environment in which a system is developed or manufactured, tested, deployed, maintained, and retired/decommissioned"[141], ENISA considers the specific supply chain reference model for IoT by framing the model into the physical aspect (all the physical objects along the supply chain phases)

---

[136] See https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/zero-day

[137] Bert Jaap Koops and Eleni Kosta, 'Looking for Some Light through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities against "Going Dark"' (2018) 34 Computer Law & Security Review 890, 898; Giovanni Ziccardi, 'The GDPR and the LIBE Study on the Use of Hacking Tools by Law Enforcement Agencies' (2018) 4 Italian Law Journal <https://heinonline.org/HOL/Page?handle=hein.journals/italj4&id=223&div=15&collection=journals> accessed 21 September 2021.

[138] Paul Stockton and Michele Golabek-Goldman, 'Curbing the Market for Cyber Weapons' (2013) 32 Yale Law & Policy Review 239 <https://digitalcommons.law.yale.edu/ylpr/vol32/iss1/11> accessed 21 September 2021.

[139] The Guardian, 'The Pegasus Project' (*2021*) <https://www.theguardian.com/news/series/pegasus-project> accessed 21 September 2021.

[140] Tope Omitola and Gary Wills, 'Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain' (2018) 126 Procedia Computer Science 441, 445.

[141] Jon Boyens and others, 'Supply Chain Risk Management Practices for Federal Information Systems and Organizations' (2015) 4 <http://dx.doi.org/10.6028/NIST.SP.800-161> accessed 20 September 2021.

and the logic aspect (software development and deployment; network-based connections and virtual interactions between IoT objects and the supply chain stakeholders)[142].

Recent discussions, both in Europe and in the US, find a consensus that supply chain security is indeed a crucial issue for IoT. ENISA and NIST acknowledge that the IoT supply chain on the one hand lays down the foundation of IoT device security, representing therefore both a challenge and an opportunity and, on the other hand raises concerns since organisations are hardly aware of the security measures adopted by market partners[143]. The guidelines published by ENISA address the IoT supply chain issue by firstly mapping out the different phases of the IoT supply chain. This serves to identify the different security threats that can arise from each phase and detail the attack scenarios. It concludes with a list of the good practices and security measures that organisations shall put in place.

As regards the supply chain reference model for IoT, 10 different stages are identified: 1) product design; 2) semiconductor fabrication (hardware); 3) component manufacturing (hardware + software); 4) component assembly & embedded software; 5) device programming (SW); 6) IoT platform development (SW); 7) service provision & end-user operation (HW + SW); 8) technical support & maintenance (HW + SW); 9) distribution and logistics (present in every stage); 10) device recovery & repurpose (HW + SW)[144]. This tenfold classification can be further divided into five different phases: conceptual phase (stage 1); development phase (stages 2-6); production phase (stage 9); utilisation phase (stage 7); support phase (stage 8); retirement phase (stage 10)[145].

Coherently with the Agency's IoT threat taxonomy, the threats have been classified under a set of high-level clusters: physical attacks (e.g., sabotage, grey markets, exploitation of inadequate physical enclosures); intellectual property loss (e.g., IP theft, reverse engineering, overproduction and cloning); nefarious activity/abuse (e.g., magnetic field attacks, malware insertion, exploitation of debug interfaces, tampering and counterfeits); legal (e.g., standard and regulation non-compliance); unintentional damage or loss of information (e.g., compromise of network, use of factory authentication settings, undetected software or hardware disruptions, user errors, disruption in cloud services, failure of recovery procedures, etc)[146]. Then, ENISA pulls the threads together by addressing the main security considerations to adopt throughout the 10 previously identified stages of the IoT

[142] ENISA, 'Guidelines for Securing the Internet of Things - Secure Supply Chain for IoT' (2020) 5.

[143] Katerina N Megas, Michael Fagan and David Lemire, 'Workshop Summary Report for "Building the Federal Profile for IoT Device Cybersecurity" Virtual Workshop NISTIR 8322' (2021) 13 <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8322.pdf> accessed 20 September 2021.

[144] ENISA, 'Guidelines for Securing the Internet of Things - Secure Supply Chain for IoT' (n 142) 12–17.

[145] ibid 9-12.

[146] ibid 18-23.

supply chain and by developing good practices for countering and mitigating the above-mentioned security threats. Specifically, good practices were classified into three clusters: actors, processes and technologies[147].

In conclusion, the report drafts a set of operational guidelines where each recommendation enucleates good practices and standards. A key condition for enhancing security is forging better relationships between relevant actors: the suggestion would then be to prioritise working with suppliers that provide cybersecurity guarantees, develop trust models and provide security promises to customers. A further step recommended by ENISA is fostering cybersecurity expertise and raising awareness within the workforce, through constant training that will promote a work culture focused on a risk-based approach. From a more technical point of view, organisations need to adopt a comprehensive, or *holistic,* approach to security. This entails adopting security by design principles, developing threat models for the supply chain, identifying third-party software, establishing a comprehensive test plan, implementing factory settings using security by default principles and leveraging existing standards and good practices[148].

1.5 Conclusion

This Chapter provided a working definition of 'Internet of Things' and 'resource-constrained devices'. In line with the definition provided by the Data Act Proposal, the IoT can be generally defined as a network of 'things', embedded with software intelligence, that obtain, generate or collect data concerning their performance, use or environment and that are able to communicate information through publicly available electronic communications services. To unravel this rather broad understanding, a three-layered IoT technical architecture taxonomy (device, network and application level) has been proposed, building on the model of Rayes and Salam, one of the most clear, comprehensive and flexible in IoT technical literature.

The IETF taxonomy of 'resource constrained devices' – based on two dimensions: computational power and memory – was then presented, as it is the most complete one. Besides the various reasons for constraints (e.g., economic, environmental, technical), the nodes on IoT networks are generally constrained in terms of computational power and/or memory, to scale up the spread of affordable and physically feasible Internet technologies. While awaiting the increase on the market of innovative technologies that promise to reduce power consumption needed for AI inference at the edge, this

[147] ibid 24-36.

[148] ibid 37-40.

work assumes that IoT systems always involve constrained technologies (typically sensors at the device layer).

Building on the IoT taxonomy, this Chapter further mapped out an IoT threat landscape by linking the specific security attacks to each layer of the model. The ENISA IoT threat taxonomy, combined with the more general ENISA threat landscapes, served as a solid foundation for this technical overview. In particular, the analysis has been supplemented by adding the main takeaways from the ENISA IoT supply chain threat taxonomy: not only does IoT architecture amplify the attack surface disproportionately, but also the compelling need to secure the supply chain across the IoT ecosystem would make the identification of a perimeter extremely challenging.

Before delving into the EU legal frameworks regulating IoT security and privacy, it is necessary to first address the different meanings of the concepts of ‘security’, ‘cybersecurity’, ‘information security’, ‘safety’ and ‘privacy’.

Chapter 2. Disentangling (Cyber)Security from the Privacy Debate in the IoT

2.1 The Concept of Cybersecurity in the IoT Era: Beyond Information Security?

With technological evolution and increasing digitalisation, the paradigms of information and computer security have changed to the point of converging into the concept – broad and transversal to different disciplines – of 'cybersecurity'[149]. In a scenario of complex interaction between information systems, society and the digital connected environment, cybersecurity takes into account a broader perimeter of risks and actors involved: as a result, new elements worthy of protection are identified. Information and computer security are now conceived as subsets of cybersecurity[150].

Information security has traditionally dealt with an understanding of security aimed at the protection of data and information[151], whilst computer security historically aimed at ensuring that systems operate as designed: the so-called CIA triad (confidentiality, integrity and availability) typical of computer security is expanded to include other principles such as non-repudiation, authenticity, accountability and auditability.

The expression 'computer security' (and its evolutions, including 'network security') refers to an original vision of information security as the protection of the computer or, more generally, of the computer system which is made up of related equipment, programmes, infrastructures and data, both processed and transmitted. Subsequently, the rise of the so-called "information society"[152] has led to the emergence of a concept of security that is more oriented towards the protection of information, namely "information security". The well-known CIA triad[153] (confidentiality, integrity and availability of the system or its components), which is central to computer security, integrates further

---

[149] Dominik Herrmann and Henning Pridöhl, 'Basic Concepts and Models of Cybersecurity' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer Science and Business Media BV 2020) 11.

[150] ENISA, 'ENISA Overview of Cybersecurity and Related Terminology Foreword by the Executive Director' (2017) 6.

[151] Michael Nieles, Kelley Dempsey and Victoria Yan Pillitteri, 'NIST Special Publication 800-12 Revision 1 - An Introduction to Information Security' (2017) <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf> accessed 31 January 2020.

[152] Frank Webster, *Theories of the Information Society* (Routledge 2014); Luciano Floridi, 'Mature Information Societies - a Matter of Expectations' (2016) 29 Philosophy & Technology 1.

[153] The CIA triad constitutes the foundation of several technical standards for computer security. See, among others, Barbara Guttman and E Roback, *An Introduction to Computer Security: The NIST Handbook, Special Publication (NIST SP)* (1995) <https://doi.org/10.6028/NIST.SP.800-12r1> or UNI/EN ISO 27001.

information security requirements to restore certainty and trust to digital relationships underpinning the continuous flows of data and information that are transformed into knowledge: non-repudiation, authenticity, accountability and verifiability[154].

From a technical and organisational perspective, computer security measures or controls are expressed in three domains: prevention, detection and response. Firstly, measures to prevent an incident and protect the system from attacks, by designing robust systems that can withstand those attacks; secondly, measures for detecting attacks or threats and ensuring the resilience of systems; finally, measures that, in response to the harmful event, aim to minimise the damage with the timely reactivation of the system and its functions. NIST's Framework identifies five concurrent and continuous security functions: Identify, Protect, Detect, Respond, Recover[155]. Each area encompasses a wide range of technical tools and organisational measures: access control, disaster recovery, encryption, hardware and software for perimeter defence, intrusion detection systems and physical security measures, etc. Prevention starts from the design phase of robust systems.

The evolution of the concept of security from computer security to information security is reflected not only in technical-scientific literature, but also in the interventions of the EU legislator. In this domain, security was initially conceived as guaranteeing the functioning of public communication networks (as early as Directive 90/387/EC on the establishment of the internal market for telecommunication services), to later arrive at a new vision focused on the protection of data and information in the European Digital Single Market strategy, where information security becomes central to fostering trust in the digital environment[156].

The next step, as shown by Veale and Brown, was the replacement, either by scientific literature or common jargon, of the more technical concepts of computer and information security with the term cybersecurity[157]. On the definition of the latter, however, a consensus has not yet been reached. Originally coined in the U.S. to refer to the ability of defending and protecting cyberspace against

---

[154] NIST, 'NISTIR 8074 - Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity', vol 2 (Michael Hogan and Elaine Newton eds, 2015) 42 <http://dx.doi.org/10.6028/NIST.IR.8074v2> accessed 4 October 2021.

[155] NIST, 'Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1' (2018) <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> accessed 4 October 2021.

[156] This approach can be found within the Regulation EU 2016/679 (General Data Protection Regulation – GDPR) and Regulation EU 91/2014 (electronic IDentification Authentication and Signature – eIDAS).

[157] Michael Veale and Ian Brown, 'Cybersecurity' (2020) 9 Internet Policy Review 1: since 2003, the concept of cybersecurity has been increasingly referred to in both academic and mainstream publications, in fields including software engineering, international relations, crisis management and public security, slowly overtaking more technical terms such as computer security, system security or data security (popular in the 1970s/80s) and information security (popular since the mid-1990s).

cyberthreats[158], the term generally refers to the necessary expansion of the "perimeter" to be protected. Limiting the concept of cybersecurity to the protection of networks and information systems alone is misleading and quite anachronistic: in the IoT era, the values and assets to be protected are much more than this.

On the one hand, faced with the challenges of increasing threats and attacks, both in quantitative and qualitative terms, cybersecurity has the objective of protecting the information systems of an organisation (institution or company) through the study, development and implementation of strategies, policies and operational plans aimed at preventing computer incidents and, when they occur, coping with and overcoming them[159]. It strives to ensure that the security properties of organisations, alongside users' assets, are maintained at a high level against relevant risks in the cyber environment. Insofar as security is about protecting organisation's assets from threats posed by attackers exploiting vulnerabilities in the system, drawing up a security plan consists of identifying and ranking the assets, identifying the threats and estimating the risks.

On the other hand, thanks also to the IoT, the risk factors in today's hyper-connected digital environment are not only linked to the underlying technological and logical infrastructure. An attack could also infringe people's rights, impair individuals' safety and freedoms, alter the political debate of a nation and, if the critical infrastructure is concerned, have serious consequences for communities, institutions and businesses. Procedures, controls and behaviours, together with technology, are the foundations of cybersecurity. In fact, it is less about adopting the latest technological product, and more about defining procedures (legislative, administrative and organisational rules), setting up control mechanisms and promoting the right individual behaviour to manage the *risk*[160]. Risk cannot be merely reduced to the individual relationship with ICTs. Rather, in certain scenarios, it concerns collective interests and affects public security.

Indeed, the increasing wave of cyberattacks has raised awareness about the vulnerability of different actors – individuals, businesses, public bodies, institutions, organisations – to cyber threats. The World Economic Forum's Global Risk Report already ranked cyberattacks among the top ten global

---

[158] Celia Paulsen and Robert Byers, *Glossary of Key Information Security Terms, NIST Interagency/Internal Report (NISTIR)* (National Institute of Standards and Technology 2019) <https://doi.org/10.6028/NIST.IR.7298r3> accessed 2 October 2021.

[159] See the technical standard UNI/EN ISO 104559.

[160] The concept of risk permeates the entire discipline of computer security. The risk is the effect of uncertainty on the security objectives of the system and, as such, can be measured in probabilistic terms as the combination of the severity of the consequences of a given dangerous event (impact) and the probability of the event itself happening (ISO 73:2009). The methodologies for the "risk control" are many; basically, the activity consists of several steps that may have different perimeters depending on the reference standard. In particular, ISO 31000 defines two steps: (i) risk assessment, which includes hazard identification, analysis and severity weighting, and (ii) risk treatment, which aims to mitigate the effects of the risk by taking appropriate measures and to verify the residual risk.

risks in 2019, and the data documented by the most recent security reports confirm said evaluation[161]. To make matters worse, a shortage of cybersecurity skills and a gap are well documented. In this respect, ENISA contributes to addressing this issue in a twofold manner. First, it "provides an overview of the current supply of cybersecurity skills in Europe through an analysis of data gathered and generated by the recently established Cybersecurity Higher Education Database (CyberHEAD). Secondly, it describes the policy approaches adopted by EU Member States in their quest to increase and sustain their national cybersecurity workforces"[162]. Moreover, the COVID-19 pandemic has forced less-prepared agents to migrate either their businesses or aspects related to personal life to the cyber dimension, resulting in a weakening of the global level of cybersecurity. Cybercriminals have started to exploit the extreme hardship experienced by some sectors – such as manufacturing and healthcare – by targeting their victims with customised attack vectors[163]. As the "2020 Year in Review" report by European Union Agency for Cybersecurity shows, cybersecurity has been faced with a paradox: it has been both the challenge and the opportunity to facilitate transformation as a confidence-building tool in digital services[164]. This ambivalent character of cybersecurity is a recurring theme of this chapter.

As addressed in Chapter 1, drawing a picture of dynamically changing threats is not an easy task. The main reason for the major cyber incidents (such as, theft of information, data and user credentials)[165] in 2020 is economic. The stolen information is usually sold on the dark web and in turn becomes a tool for other types of attacks, such as financial fraud or espionage and sabotage, aimed at acquiring industrial, commercial or expert information, driving companies out of business and causing reputational and organisational damage. The crime-as-a-service model is increasingly acquiring relevance: criminal organisations structured as companies offer ready-to-use software that does not require any particular computer skills to perpetrate attacks[166].

---

[161] World Economic Forum, 'The Global Risks Report 2021' (2021) <https://www.weforum.org/reports/the-global-risks-report-2021> accessed 2 October 2021.

[162] ENISA, 'Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education' (2021) <https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education> accessed 27 November 2021.

[163] EUROPOL, 'Internet Organised Crime Threat Assessment (IOCTA)' (2020) <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020> accessed 2 October 2021.

[164] ENISA, 'The Year in Review ENISA Threat Landscape - From January 2019 to April 2020' (2020) <https://www.thehaguesecuritydelta.com/media/com_hsd/report/337/document/ETL2020-A-year-in-review-A4-4-.pdf> accessed 2 October 2021.

[165] A computer incident is any event of a malicious or negligent nature intended to damage tangible, intangible and human resources of value to the system or organisation. A computer incident therefore means not only 'hacker attacks' or external intrusions, but also inappropriate behaviour by system users, equipment failure, software bugs or natural events and disasters.

[166] Derek Manky, 'Cybercrime as a Service: A Very Modern Business' (2013) 2013 Computer Fraud & Security 9.

However, these threats are part of a bigger picture of concern. A relatively new and problematic dimension is related to cyberwar[167] and information warfare[168], where conflict between states is conducted through cyberattacks on various types of information systems, national critical infrastructures and services whose malfunctioning causes disruptions. Politics and social life are directly affected by the spreading of fake news, trolls and manipulated information on the web and amplified by social networks[169]. The control of information through security technologies does not only concern criminal law, but also administrative, private and European law[170]: cybersecurity intersects all these different traditional legal domains.

Moreover, new challenges arise from the malicious use of artificial intelligence (AI). AI offers new and more effective ways of conducting cyberattacks. These systems are able to identify vulnerabilities that may escape human expertise; they facilitate automated personalised, social engineering attacks using information gathered online; they generate images and videos that cannot be distinguished from reality (so-called deep fakes); they create malware which are autonomous in masquerading and selecting their target; or they attack other AI systems by adversely applying the same machine-learning paradigms[171].

The attacks are based on the ever-increasing security gaps in information systems, but they also succeed by exploiting the so-called "human factor". A country's overall level of cybersecurity preparedness depends not only on the level of security of public and private sector organisations, but also on the security knowledge of individual users who can be leveraged as attack vectors on institutions or critical infrastructures[172]. The extent to which an individual is vulnerable largely depends on the risk perception and the degree of technical competence. The risks arising from

---

[167] Jonathan F Lancelot, 'Cyber-Diplomacy: Cyberwarfare and the Rules of Engagement' (2020) 4 Journal of Cyber Security Technology 240 <https://www.tandfonline.com/doi/abs/10.1080/23742917.2020.1798155> accessed 2 October 2021.

[168] Fabio Rugge, 'Mind Hacking: La Guerra Informativa Nell'era Cyber' (2018) 34 Notizie di Politeia 108.

[169] Giovanni Ziccardi, *Tecnologie per Il Potere: Come Usare i Social Network in Politica* (Raffaello Cortina Editore 2019). Harmful behaviour such as harassment, hatred, bullying and stalking has a strong potential to damage reputations in the online dimension due to the persistence of information and its potential to go viral. Identity theft, often facilitated by security gaps, can become a tool not only for committing fraud and scams, but also for defamation offences and disseminating confidential content for revenge (revenge porn) or extortion and blackmail (sexstortion) and persecution of vulnerable individuals. See Danielle Citron and Mary Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest Law Review <https://digitalcommons.law.umaryland.edu/fac_pubs/1420> accessed 2 October 2021; Giovanni Ziccardi, *L'odio Online: Violenza Verbale e Ossessioni in Rete* (Raffaello Cortina Editore 2016).

[170] Mark D Cole, Christina Etteldorf and Carsten Ullrich, *Cross-Border Dissemination of Online Content*, vol 81 (1st edn, Nomos Verlagsgesellschaft mbH & Co KG 2020) <https://doi.org/10.5771/9783748906438,> accessed 4 October 2021; Alessandro Mantelero and others, 'The Common EU Approach to Personal Data and Cybersecurity Regulation' (2021) 28 International Journal of Law and Information Technology 297 <https://academic.oup.com/ijlit/article/28/4/297/6120059> accessed 4 October 2021.

[171] ENISA, 'Artificial Intelligence Threat Landscape Report ' (n 128).

[172] The next section addresses the concept of "computer hygiene" which emphasises consumers' responsibilities.

personal data misuse[173], with severe consequences to the construction of personal identity[174], online reputation and exposure to cybercrime[175], are often overlooked. In this respect, traditional threat models, as seen in section 1.4, and attackers' profiles[176] may be limited.

Against this backdrop, the European Union has been contributing to a new conceptualisation of cybersecurity since 2013, when the "European Union Strategy for Cybersecurity: An Open and Secure Cyberspace" (the so-called Cybersecurity Strategy) was published. With a top-down approach, the Union recalls that a high level of cybersecurity is necessary, not only to maintain essential services and for the functioning of society and the economy, but also to safeguard citizens' safety. The NIS Directive (Directive EU 2016/1148) – the first piece of EU legislation on this matter – was meant to define common standards for cybersecurity, 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 or stored or transmitted or processed data or the related services offered by, or accessible via, those network or information systems"[177].

The project for a more resilient European Union to cyberthreats was relaunched with a series of measures proposed by the Commission in 2017 to fill the gaps in the already existing rules and to strengthen the 2013 strategy with a view to making cybersecurity a harmonised subject at EU level. In particular, the EU adopted Regulation EU 881/2019 (Cybersecurity Act)[178], which entered into force on 27 June 2019. It consists of two parts: in the first, the role of ENISA is specified and enhanced. ENISA – which played a mere role of technical advisor to Member States in the event of cyberattacks or incidents – takes on an operational role in the management of cyberthreats, ensuring that the response to attacks of this nature (which has always been the prerogative of Member States) has communitarian relevance and is managed at supranational level. In the second part, the Regulation introduces the creation of a common European framework for certifying the cybersecurity of ICT

---

[173] Michele Martoni, 'Datificazione Dei Nativi Digitali e Società Della Classificazione. Prime Riflessioni Sull'educazione Alla Cittadinanza Digitale' (2020) 1 Federalismi.it 119 <https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=40849> accessed 2 October 2021.

[174] Palmirani and Martoni (n 8).

[175] Raffaella Brighi, 'Cibercrimine e Anonimato in Rete. Riflessioni Su Sicurezza, Efficacia Investigativa e Tutela Delle Libertà Personali' [2017] Sicurezza e Scienze Sociali 29 <http://www.francoangeli.it/Riviste/SchedaRivista.aspx?IDarticolo=61321&lingua=IT> accessed 2 October 2021.

[176] For example, family members or acquaintances are not considered as possible attackers, even though they benefit from easy access to the victim's devices in an abusive context.

[177] Directive EU 2016/1148, Article 4(2); this concept is defined in the very same terms in the so-called ENISA regulation 526/2013.

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

products and digital services, with the aim of facilitating their exchange within the EU and increasing consumer trust.

The Cybersecurity Act proposes a definition of cybersecurity that is deliberately much broader than previous ones, which includes all the "activities necessary to protect network and information systems, the users of these systems and other persons affected by cyberthreats" [179]. The notion was intentionally left as a broad one by the European legislator in order to encompass a broad range of governance risks without conceptualising it in an unduly limited fashion[180]. The new EU cybersecurity strategy, which was presented by the Commission in December 2020, completes the journey by introducing various proposals for the enforcement of a coherent legal, political and investment framework to address the current challenges. Chapter 3 provides an in-depth analysis of the EU legal frameworks regulating cybersecurity in the IoT domain.

All in all, in complex environments of interaction between people, physical devices, software and services, cybersecurity calls for a holistic approach that integrates the protection of the many values at stake in new coordinated forms of risk management. This may explain why, unlike more technical terms such as *computer security* and *information security,* there is no shared notion of cybersecurity, let alone defined boundaries at any level i.e., scientific, political and doctrinal. As acknowledged by Fuster and Jasmontaite, the resulting evolving and highly fragmented field of cybersecurity is a horizontal problem, "which is in a sense a common denominator of various new technologies connected to the World Wide Web"[181].

The IoT, as repeatedly stressed in this work, is a game-changer. And cybersecurity makes no exception. As seen in Chapter 1, the ubiquitous data and metadata sharing of these systems, which play an increasingly important role both in the public and the private dimension, implies a paradigm shift. The security of a network relies on the security of each of its components. Therefore, the (cyber)security of IoT devices is not just about them, but *it is influenced by and has a direct impact* on every other device, service, platform and online information resource, be it virtual or physical connected. In the words of Denardis,

"[C]ybersecurity has now become one of the most consequential issues of the modern era, necessary for human safety, privacy, critical infrastructure, and national security, as much as for economic

---

[179] Art. 2, Regulation EU 2019/881

[180] Gloria González Fuster and Lina Jasmontaite, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer, Cham 2020) 103 <https://link.springer.com/chapter/10.1007/978-3-030-29053-5_5> accessed 2 October 2021.

[181] ibid 98.

security, democracy, speech rights, and access to knowledge. Yet connected physical objects are notoriously insecure. There is a huge chasm between the need for security and the state of security."[182]

In the digital era, a functional definition of security shall necessarily weight the broad notion of cybersecurity, in order to sharpen the focus on the private sphere. Against the background where many cybersecurity objectives coincide with the common interest, the following sections of the Chapter aim at casting light on how the interplay between cybersecurity, fundamental rights (i.e., privacy and data protection) and individual safety works in the context of IoT resource-constrained devices. The question is whether and to what extent cybersecurity values and practices *always* facilitate or protect the integrity of individuals (the moral value of individual safety) and the enjoyment of the fundamental rights to privacy and to data protection. In other words, this relates to the quandary of whether "security is, like privacy, a human right or rather a precondition for the legal framework on which effective human rights depend"[183].

2.2 The Relationship between Cybersecurity, Privacy & Data Protection and Safety

2.2.1 Privacy and data protection in the EU: a brief background

The right to privacy – or the right to respect for private life – emerged in international human rights law in the aftermath of World War II. First of all, in the Universal Declaration of Human Rights (UDHR), adopted in 1948[184], and soon after in the European Convention on Human Rights (ECHR), adopted in 1950 by the Council of Europe (CoE)[185]. The ECHR provides that everyone has the right to respect for his or her private and family life, home and correspondence[186]. Albeit Article 8 of the ECHR lays down a general prohibition of interference by a public authority, it is not absolute: interference is permitted if in accordance with the law, pursues legitimate public interests (such as national security and public safety) and is necessary in a democratic society[187].

---

[182] Denardis (n 17) 7.

[183] Mireille Hildebrandt, 'Digital Security and Human Rights: A Plea for Counter-Infringement Measures' in Mart Susi (ed), *Human Rights, Digital Society and the Law* (1st edn, Routledge 2019) 266.

[184] Article 12 of the Universal Declaration of Human Rights: "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".

[185] The Convention is legally binding on the contracting parties. CoE established in France (Strasburg), in 1959, the European Court of Human Rights (ECtHR) to ensure that contracting parties observed the obligations enshrined in the Convention. The ECtHR considers complaints from individuals, groups, NGOs or legal persons bring forward as violations of the convention. The ECtHR can also examine inter-state cases brought by one or more CoE member states against another member state.

[186] Article 8 para 1, ECHR.

[187] Article 8 para 2, ECHR.

As the emergence of information technology in the 1960s and 1970s clearly showed an urgent need for more detailed rules to safeguard individuals' personal data, the Committee of Ministers of the CoE adopted various resolutions on personal data protection, on the basis of Article 8 of the ECHR[188]. In 1981, the Council of Europe opened a Convention for the protection of individuals for signature, that regarded the automatic processing of personal data (Convention 108). The possibility to sign and ratify the Convention was extended to non-contracting parties of the CoE in order to promote a high data protection standard on a global level. Convention 108 applies to all data processing carried out by both the private and public sectors, including data processing by the judiciary and law enforcement authorities. Although outside the judicial supervision of the ECtHR, the Strasburg Court has taken Convention 108 into consideration in its case law in determining whether or not there has been an interference with Article 8 of the ECHR[189].

As regards EU primary law, the Charter of Fundamental Rights of the European Union[190] (hereinafter, the "Charter")[191] became legally binding when the Lisbon Treaty came into force on 1 December 2009. The Charter clearly envisioned these two rights in a separate fashion, making a distinction between the traditional right to respect for one's private and family life (art. 7) and the right to the protection of personal data (art. 8)[192]. The right to privacy is indeed closely related to the right to data protection.

On the one hand, both aim to protect similar fundamental values i.e., the *autonomy* and *human dignity* of people, by granting them a personal sphere in which they can freely develop their personality and shape their opinions and ideas[193]. In other words, an essential infrastructure for liberal democratic political systems[194]. Floridi, who has re-interpreted the informational privacy theory in light of the

---

[188] European Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor, *Handbook on European Data Protection Law* (Publications Office of the European Union 2018) 24.

[189] ECtHR, 25 February 1997, (Application No. 22009/93), *Z v. Finland*.

[190] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 40) 28: "[i]t incorporates the whole range of civil, political, economic and social rights of European citizens, by synthesising the constitutional traditions and international obligations common to the Member States. The rights described in the Charter are divided into six sections: dignity, freedoms, equality, solidarity, citizens' rights and justice".

[191] EU (2012), Charter of Fundamental Rights of the European Union, OJ 2012 C 326.

[192] Opinion of AG Sharpston, 27 September 2018, Case C 345/17, *Buivids,* ECLI:EU:C:2018:780, § 61: the case law of the European Court of Human Rights (ECtHR) has substantially included the fundamental right to personal data protection within the scope of Article 8 ECHR, by "treating it as a more specific expression of the right to privacy in respect of the processing of personal data".

[193] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 188) 20–21.

[194] Julie E Cohen, 'What Privacy Is For' (2013) 126 Harvard Law Review 1904, 1905 <https://www.jstor.org/stable/23415061> accessed 7 October 2021.

digital revolution[195], conceptualises an *anthropo-eccentrical* understanding of human exceptionalism – which, in the history of philosophy, provided for various interpretations of the concept of human dignity – to highlight the right to privacy based on human dignity[196]. Indeed, the EU approach emphasises an understanding of dignity – enshrined in Article 1 of the EU Charter of Fundamental Rights – which combines intimacy with respect, two dimensions of privacy, while contributing to defining the position of each person in society[197]. Yet, human dignity is also central to personal data protection[198], and more generally to the evolution experienced by domestic jurisdictions[199]. "One can therefore come to the conclusion that dignity is a universal, fundamental, and inescapable term of reference"[200].

On the other hand, despite substantial overlaps, these rights have different scopes and rationales[201]. The right to personal data protection comes into play whenever personal data are processed, whereas the right to privacy concerns situations where a private interest, or the "private life" of an individual, has been compromised. A more traditional, and rather sharp, distinction would contrast a 'classic' right (the right to respect for private life), revolving around a general prohibition on interference, with a more 'modern' one (the right to personal data protection), setting up a model of checks and balances to safeguard individuals when their personal data are processed, as claimed by Advocate General Sharpston in *Volker und Markus Schecke*[202]. Several authors, such as Pagallo, Gutwirth and De Hert,

---

[195] Luciano Floridi, 'The Ontological Interpretation of Informational Privacy' (2005) 7 Ethics and Information Technology 185, 194: a new theoretical paradigm has to put the "essentially informational nature of human beings and of their operations as informational social agents" at the heart of the privacy debate. Each person, *rectius*: each agent, is her information. A breach of one's informational privacy is a form of aggression towards one's personal identity: the ontological interpretation relies on the equalisation of the informational sphere and the personal identity. It follows that informational privacy might be conceived as a function of ontological friction, namely the forces that contrast the flow of information in each environment (or a region of the infosphere). In other words, this friction is the effort that an agent must make in order to gain information about others entity in the same infosphere. This expectation of privacy is well suited to dispose of the "false dichotomy qualifying informational privacy in public or in private contexts".

[196] Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 Philosophy & Technology 307 <https://link.springer.com/article/10.1007/s13347-016-0220-8> accessed 7 October 2021.

[197] Stefano Rodotà, 'Privacy, Libertà, Dignità - Privacy, Freedom, and Dignity', *Conclusive Remarks at the 26th International Conference on Privacy and Data Protection* (2004) 7 <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293> accessed 6 October 2021.

[198] Article 88 of the General Data Protection Regulation (GDPR) states that rules "shall include suitable and specific measures to safeguard the data subject's human dignity [my italics], legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work-place".

[199] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).

[200] Rodotà (n 197) 7.

[201] Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222; Deni Elliott, 'Data Protection Is More than Privacy' (2019) 5 European Data Protection Law Review 13; Orla Lynskey, 'Deconstructing Data Protection: The "added-Value" of a Right to Data Protection in the Eu Legal Order' (2014) 63 International and Comparative Law Quarterly 569.

[202] Opinion of AG Sharpston, 17 June 2010, Join cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen.

conceive the relation between the two in terms of protection of individuals' "opaqueness" *versus* the "transparency" of the collection and processing of personal data[203]. Whereas privacy refers to the holistic intertemporal protection of an individual's inner dimensions, (personal) data protection rights, triggered when people begin to allow information to leave that private sphere, aim at demanding the transparency of such processing.

Notwithstanding the soundness of the above-mentioned distinctions, as noted by Fuster and Hijmans, "the two rights are clearly coupled in the relevant case law of the Court of Justice of the European Union (CJEU), where they are not *systematically* distinguished – and where they are occasionally presented in complex interwoven manners"[204]. Moreover, "place is no longer a useful proxy to delineate the boundaries of the private sphere"[205]. Accordingly, (informational) privacy would then come closer to data protection provided that the latter does not make "any crucial private/public distinction"[206]. In a closer look, this interpretation echoes the 'revolutionary' scope of the right to data protection *à la européenne*, namely the recognition all citizens to have permanent power of *management* over their data, wherever they may be. The term 'management' is more nuanced when it comes to conceptualizing the problematic concept of 'control' within traditional informational

[203] Serge Gutwirth and Paul De Hert, 'Regulating Profiling in a Democratic Constitutional State' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008) 271; Ugo Pagallo, 'The Group, the Private, and the Individual: A New Level of Data Protection?' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy* (Springer 2017) 159.

[204] Gloria González Fuster and Hijmans Hielke, 'The EU Rights to Privacy and Personal Data Protection: 20 Years in 10 Questions - Discussion Paper', *International Workshop 'Exploring the Privacy and Data Protection connection: International Workshop on the Legal Notions of Privacy and Data Protection in EU Law in a Rapidly Changing World'* (2019) 4 <https://brusselsprivacyhub.eu/events/20190513.Working_Paper_González_Fuster_Hijmans.pdf> accessed 31 January 2020. see also Case C-73/16, *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej* správy [2017] ECLI:EU:C:2017:253, §112: "the protection of the fundamental right to respect for private life at the European Union level requires that derogations from the protection of personal data and its limitations be carried out within the limits of what is strictly necessary".

[205] See *ex multis* Bert-Jaap Koops, 'On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy' (2014) 3 Politica e Società 247, 7. See also ECtHR, 24 June 2004, (Application no 59320/00) *von Hannover v Germany*: the Strasbourg Court held that in a case concerning the interception of telephone calls on business premises, the applicant "would have had a reasonable expectation of privacy for such calls".

[206] Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2 European Data Protection Law Review 43: the author highlights that in Lindqvist Case C-101/01 and in Rynes Case C- 212/13 the Court of Luxembourg acknowledged the "house-hold" processing exemption, that is indeed space-dependent, more as a de minimis principle than a spatial one.

privacy theories[207]. The accountability principle[208] can thus be seen as a fundamental lever[209] through which individuals can demand controllers to demonstrate compliance with the EU principles and rights related to the processing of personal data. It is worth noting that this *data management power* is also delegated to independent authorities[210]: protection is no longer merely individualistic but involves a specific public responsibility. Chapter 4 will further address the main legal challenges in terms of EU privacy and data protection legal frameworks brought about by IoT structural data and metadata sharing.

2.2.2 Cybersecurity and Privacy: an instrumental, or infraethical, perspective

The multifaceted relationship between security and privacy raises the long-standing question, which has long been a concern within the moral theory and the legal scholarly debate, about whether these values are weighted in terms of trade-offs or balances, when pursuing the aims of the former lead to infringe the latter. In the attempt to clarify this conundrum, this section discusses the tripartite theoretical model of Hildebrandt[211], which paradoxically assumes that digital security technologies generate new cybersecurity risks as well as violations of fundamental rights[212].

The legal-philosophical analysis needs to preliminary assess the cases where security and fundamental rights are on the same level, and thus need to be balanced, and where one is conditional, or instrumental, for the other. To do so, Floridi's theory of infraethics comes to our aid[213].

At the end of July 2020, the EU Commission presented the "European Security Strategy 2020-2025". The programmatic opening makes clear the ultimate value of the strategy: protecting individuals, society and the environment. But even more important, for the purpose of this study, is the following statement: "security is not only the basis for personal safety, it also protects fundamental rights and provides the foundation for confidence and dynamism in our economy, our society and our

---

[207] Lita Van Wel and Lambèr Royakkers, 'Ethical Issues in Web Data Mining' (2004) 6 Ethics and Information Technology 129, 130–140 <https://link.springer.com/article/10.1023/B:ETIN.0000047476.05912.3d> accessed 16 March 2022; Brent Daniel Mittelstadt and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 Big Data and Society 205395171667967, 9–10 <http://journals.sagepub.com/doi/10.1177/2053951716679679> accessed 31 March 2020; Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 Northwestern Journal of Technology and Intellectual Property 239 <https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1> accessed 3 March 2020; Bart W Schermer, 'The Limits of Privacy in Automated Profiling and Data Mining' (2011) 27 Computer Law and Security Review 45, 45–52.

[208] Art. 5(2), Regulation (EU) 2016/679.

[209] Ugo Pagallo, Pompeu Casanovas and Robert Madelin, 'The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data' (2019) 7 Theory and Practice of Legislation 1.

[210] Art. 8(3), Charter of Fundamental Rights of the European Union.

[211] Hildebrandt (n 183).

[212] ibid 264.

[213] Luciano Floridi, 'Infraethics–on the Conditions of Possibility of Morality' (2017) 30 Philosophy & Technology 391 <https://link.springer.com/article/10.1007/s13347-017-0291-1> accessed 8 October 2021.

democracy"[214]. The phrasing of the Commission seems to offer a key to interpreting the perennial philosophical debate around security within moral theory, namely whether security has itself an ethical dimension (thus, a fundamental good) or, rather, it is a precondition for the legal framework on which effective human rights depend.

In the words of the Commission, terms such as *basis* and *foundation* suggest that the tension between security, on one side, and safety or fundamental rights (e.g., privacy and data protection), on the other, might not be dealt with as a balance within ethics, or rather moral rights on the same level. Rather, as suggested by Floridi, the balance that needs to be attained is between '*infraethics*' (security as an instrumental value) and ethics (safety or privacy, as fundamental goods)[215]. By infraethics, the philosopher from Oxford means a not-yet-ethical framework, that is, a "set of conditions that facilitate or hinder evaluations, decisions, actions, or situations, which are then moral or immoral"[216]. In other words, whereas ethics governs the axiological evaluation of a state of affairs[217], "the right sort of infraethics is there to support the right kind of axiology"[218] of morally good values, such as fundamental rights (privacy) or personal safety.

There were others that also acknowledged the *instrumental* character of cybersecurity vis-à-vis moral values[219]. Thus, as Jabri emphasised, "the point at which security is transformed into a universal ethical category is also the point at which it becomes a technology of domination, of the governing over the governed"[220]. Therefore, we assume that cybersecurity and its technologies, viewed within an infraethical perspective – which is not ethically neutral, may either facilitate or hinder morally good values: fundamental rights and individual safety.

Before embarking on the intricate conundrum of cybersecurity technologies that may hinder fundamental rights two caveats apply. On the one hand, this section will not dwell too extensively on

---

[214] European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy' (2020) 1 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605> accessed 6 October 2021.

[215] Luciano Floridi, "Infraethics–on the Conditions of Possibility of Morality" (2017) 30 Philosophy & Technology, 394.

[216] Floridi, 'Infraethics–on the Conditions of Possibility of Morality' (n 213) 392.

[217] Massimo Durante, *Ethics, Law and the Politics of Information: A Guide to the Philosophy of Luciano Floridi*, vol 18 (Springer Netherlands 2017) 176–177 <http://link.springer.com/10.1007/978-94-024-1150-8> accessed 8 October 2021.

[218] Floridi, 'Infraethics–on the Conditions of Possibility of Morality' (n 213) 397.

[219] Michele Loi and Markus Christen, 'Ethical Frameworks for Cybersecurity' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer Science and Business Media BV 2020) 76; *contra* see Ibo van de Poel, 'Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer Science and Business Media BV 2020).

[220] Vivienne Jabri, 'Security: Critique, Analysis and Ethics' in Jonna Nyman and Anthony Burke (eds), *Ethical security studies : a new research agenda* (Routledge 2016) 27.

the limitations of the scope of EU fundamental rights law (i.e., the Charter) and international human rights law (i.e., the ECHR), and the caselaw of the CJEU and the ECtHR respectively, since a more in-depth reflection on the challenges brought by the IoT in terms of balances between EU privacy and data protection legal frameworks and security will be addressed later in Chapter 4. On the other hand, it does not follow a moral judgement, as suggested by Floridi, of the circumstances where cybersecurity technologies infringe fundamental rights. Rather, the infraethics, here, is seen through the lens of Hildebrandt's model: when it becomes necessary to weigh *cybersecurity-as-a-fundamental-good* and other fundamental goods, such as privacy, a "bad infraethics" applies trade-offs rather than balances. A balancing act implies that the higher the infringement of fundamental rights, the more effective safeguards must be implemented[221].

It is worth recalling in this regard two of the three dimensions of cybersecurity, as outlined in section 2.1. These are resilience and response, the 'active face' of digital security. Systems resilience is achieved by deploying so-called detection technologies and controls. These include: (i) procedures for analysing log files; (ii) procedures for monitoring network traffic and possible anomalies on the systems, implemented through sophisticated tools such as Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM)[222]. Conversely, the response (to attacks) is mainly based on autonomous and semi-autonomous measures as pre-determined responses for a number of threats. They span from advanced backups, disaster recovery procedures and tools to business continuity plans, relying on distributed network architectures and redundant systems[223].

These two domains of cybersecurity substantially overlap with the second and the third type of digital security technologies (DTSs) described by Hildebrandt. The former aims to detect and counter threats and vulnerabilities in digital environments, thus including monitoring, filtering and blocking technologies. The latter aims to detect and counter cybercrime, thus concerning the power of law-enforcement agencies to search and seize stored digital data, to collect and intercept digital data in real time[224]. Undoubtedly, in these instances, cybersecurity technologies pose serious risks of undermining and breaching users' fundamental rights to privacy and data protection, and users' exposure to extra risks, should data confidentiality be breached, and may have a mass-surveillance effect[225].

---

[221] Hildebrandt (n 183) 270.

[222] Raffaella Brighi, 'Cybersecurity. Dimensione Pubblica e Privata Della Sicurezza Dei Dati' in Thomas Casadei and Stefano Pietropaoli (eds), *Diritto e Tecnologie Informatiche - Questioni di Informatica Giuridica, Prospettive Istituzionali e Sfide Sociali* (Cedam 2021) 140.

[223] ibid.

[224] Hildebrandt (n 183) 263.

[225] Mariarosaria Taddeo, 'Is Cybersecurity a Public Good?' (2019) 29 Minds and Machines 349, 353.

In the context of human rights law, Article 8(2) ECHR provides for a general prohibition of State interference with the right to respect for private and family life, *except* when the infringement "is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing 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"[226].

The balancing act requires a solid legal justification: the infringing measure has to be (i) in accordance with the law; (ii) necessary in a democratic society; (iii) with a legitimate aim. In the case law of ECtHR[227], the lawfulness criterion is interpreted as requiring the national law to be sufficiently clear in its terms (adequately accessible) to give everyone an indication as to the circumstances in which and the conditions on which (sufficiently foreseeable) public authorities are empowered to resort to such infringing measures and contains effective safeguards in order to limit such measures either in scope (time and content) or scale[228].

Hildebrandt therefore concludes that:

> "*[a] more effective level of digital security is a necessary but not a sufficient condition for giving up some privacy, also taking into account that the more privacy invasive a DST the higher the threshold should be for allowing it. If security threats and proportionate DSTs meet the threshold of a sufficient condition, a balance must be struck: the higher the infringement of human rights, the more effective safeguards must be implemented. In line with data protection by design and default, human rights law must develop the notion of counter-infringement measures as part of the necessary safeguards under human rights law. Like data protection by design this would be another instance of legal protection by design"*[229].

Similarly, in its case-law on surveillance[230], the CJEU assesses the strength of the safeguards embedded in EU and national law for the rights to privacy and data protection vis-à-vis the monitoring activities of State law enforcement agencies. The EU law, and in particular Article 15(1) of the ePrivacy Directive, authorises Member States to derogate to some of the security and confidentiality requirements set out in the Directive when such restriction constitutes a necessary, appropriate and

---

[226] ECHR, Article 8(2).

[227] ECtHR, 28 November 2002, (Application no. 58442/00), *Lavents v. Latvia*, §135.

[228] European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights* (Council of Europe 2021) 108.

[229] Hildebrandt (n 183) 270.

[230] Case C-623/17, *Privacy International* [2020] ECLI:EU:*C*:2020:790*;* Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson and Others* [2016] ECLI:EU:C:2016:970.

proportionate measure within a democratic society to safeguard national security (i.e., State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system[231]. Chapter 4 will further elaborate on the recent CJEU and ECtHR case-law on surveillance, which offers useful insights into how security goals can be proportionally achieved while respecting the rights to privacy and data protection.

The other understanding of *cybersecurity-as-infraethics*, that is, a good infraethics, is meant as a condition of the possibility for fundamental rights and individual safety, without involving any kind of balancing act. The first dimension of cybersecurity i.e., system robustness, focuses on building solid, reliable systems that can withstand and mitigate attacks. Its 'passive character' is essential for understanding why it is not problematic for fundamental rights.

In the era of IoT ubiquitous hyper-connectedness, system robustness has direct implications on the public interest of information societies, for it benefits all users of the network without possibility of exclusion[232]. It enables critical national infrastructures and services to function and it allows citizens to rely on, or trust, secure IoT technologies since cybersecurity requirements – framed in terms of system robustness – are "essential component[s] of the protection of individuals with regard to the processing of personal data"[233].

Indeed, this instrumental value of security is also acknowledged by the GDPR, whose broad scope is made clear by Article 1(2)[234]. Security is one of the core principles around which the framework of protection is based, as per Article 5(1)(f). Article 32 then lays down a general security obligation for both data controllers and processors to implement technical and organisational measures appropriate to the risk of the processing. In other terms, Article 32 directly implements infraethics to prevent processing in infringement of the Regulation[235] and, indirectly, to uphold fundamental primary goods i.e., rights and freedoms[236].

---

[231] Directive 2002/58/EU, Article 15(1).

[232] Taddeo (n 225) 350.

[233] Nóra Ni Loideain, 'A Port in the Data-Sharing Storm: The GDPR and the Internet of Things' (2019) 4 Journal of Cyber Policy 178, 11 <https://www.tandfonline.com/doi/abs/10.1080/23738871.2019.1635176> accessed 8 October 2021.

[234] Regulation (EU) 2016/679, Article 1(2): the Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

[235] Regulation (EU) 2016/679, Recital 83.

[236] Article 32 GDPR is indeed the *trait-d'union* between legal and technical aspects of data security: it enforces legal obligations on data controllers to ensure the security of processing, by implementing technical and organisational measures appropriate for the level of the risk of the processing. A preliminary step is therefore to assess the (level of) risk. Risk methodologies (Chapter 5), in our digital era, are also strictly connected with safety (section 2.4): practitioners aim to assess the weaknesses of systems by ranking the impact of the harmful event in connection with the probability of

As noted by Burton, the CJEU seemingly made an equation between data security principles and the essence of the right to data protection[237] in *Digital Rights Ireland*[238]. Similarly, in *Z v Finland*, the ECtHR maintained that national law must ensure appropriate (security) safeguards to be consistent with Article 8 ECHR[239]. The EU security strategy acknowledges that cooperation between ENISA, data protection authorities and the European Data Protection Board is of the utmost importance to fulfil the most important long-term need of developing a culture of cybersecurity by design[240]: "security (including cybersecurity) and data protection by design are key elements to be considered under the GDPR and would benefit from a common and ambitious approach throughout the EU"[241]. Although the security requirements laid down in Article 32 GDPR apply at the time of processing, whereas the duty under Article 25 apply beforehand when the controller determines the means for processing[242], these obligations are closely linked. Data protection by design and by default principles dictate to data controllers to implement appropriate technical and organisational measures that integrate the requirements of the Regulation, including data security[243].

The design of robust systems is achieved by deploying so-called prevention measures or controls, including measures for the control of physical and logical access (such as strong passwords, smart cards, biometrics); the adoption of perimeter defence tools (such as firewalls and proxies); the definition of policies for timely updates; the provision of procedures for the definitive deletion of data and lastly, the promotion of user's awareness through constant trainings[244].

---

their occurrence. However, a necessary remark acknowledge that while the risks assessment is classically known in IT security, the data protection perspective is very different. GDPR and ISO/IEC risk analysis models differ to the extent that the former safeguards rights and freedoms of individuals, whilst the latter aims to protect corporate assets and are in general focused on risks based on which financial or reputation damage for the company could be expected. This understanding, later addressed in Chapter 5, does not necessarily imply a clash between the two: by securing organisations' assets, individuals can also be protected.

[237] Cédric Burton, 'Article 32 Security of Processing' in Christopher; Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 634.

[238] *Digital Rights Ireland* (n 230), para. 40: "Nor […] Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/ 46 and 2002/ 58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks".

[239] ECtHR, 25 February 1997, (Application no. 22009/93), *Z v Finland*, paras. 95-96.

[240] European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy' (n 214) 8.

[241] European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation COM/2020' (2020) 10 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> accessed 12 October 2021.

[242] Lee A Bygrave, 'Article 25 Data Protection by Design and by Default' in Christopher; Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 576.

[243] ENISA, 'Recommendations on Shaping Technology According to GDPR Provisions' (2018) 19.

[244] Brighi (n 222) 140.

Against the background of prevention, cryptographic technologies – such as encryption – are widely considered to be technical measures that effectively safeguard and promote fundamental rights such as the right to privacy, data protection and freedom of expression[245]. Hildebrandt, while dwelling on the digital security technologies that afford violations of fundamental rights, lists encryption within the first type of DSTs (i.e., the ones that ensure confidentiality). While the philosopher acknowledges that encryption, in principle, does not infringe fundamental rights, she argues that cryptographic techniques nonetheless generate new vulnerabilities by elaborating on their dependency on trusted parties for key management and certification[246].

It can be argued, however, that these weaknesses can be mitigated *via* technical solutions[247]. As further explored in Chapter 4, to increase trust, while avoiding potential collusions, a decentralised re-keying scheme[248] allows for the data subject to take total control over the generation and management of the decryption keys without relying on a trusted authority[249]: if two or more parties (e.g., Cloud service providers) combine the keys, they cannot decrypt data[250]. Thus, there is much thriving literature confirming that secret sharing algorithms can be successfully applied either to distribute the encryption key among a number of cloud nodes[251] or to divide a data subject's encrypted data into shares to be stored in different cloud service providers[252].

---

[245] Regulation (EU) 2016/679, article 32(1)(a); European Commission High Level Group of Scientific Adivisors, 'Cybersecurity in the European Digital Single Market' (2017) 31 <https://portal-cdn.scnat.ch/asset/ed5ae04c-1d2c-5c4f-a961-0b050fe0aa50/SAM_Cybersecurity_scientific_opinion.pdf?b=79e9c1e8-989d-5e60-a3b6-4d891f883626&v=346b7cdc-8d1b-56b5-b9b8-f270a609de88_0&s=E3AVFGsn1eZLAAjXDYG5mEbvy0RFNJHp7BK9RTe-k2WeglibkB5lzU41kidSWMNZfJlZ2zM_jwzYiPB90V-sErEZal-eqg5qbj7FWIoMhL1Uv1-HM1Osx_aKDys2tahJsdjTb7sLxNRqg3ItHewOUuBsAUnkPHs52BtJ3oGgo9E> accessed 8 October 2021; ENISA, 'ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards Our Digital Identity' (2016) 5 <www.enisa.europa.eu> accessed 8 October 2021; Wojciech Wiewiórowski, 'Keynote: Data Protection Needs Encryption, EDPS 1st Online IPEN Workshop' (2020).

[246] Hildebrandt (n 183) 262.

[247] Pier Giorgio Chiara, 'Disentangling Encryption from the Personalization Debate: On the Advisability of Endorsing the "Relativist Approach" Underpinning the Identifiability Criterion' (2020) 4 University of Vienna Law Review 168.

[248] Michael Egorov, Maclane Wilkison and Nucypher David Nuñez, 'NuCypher KMS: Decentralized Key Management System'.

[249] Tayssir Ismail and others, 'Hybrid and Secure E-Health Data Sharing Architecture in Multi-Clouds Environment', *ICOST 2020: The Impact of Digital Technologies on Public Health in Developed and Developing Countries*, vol 12157 LNCS (Springer, Cham 2020) 257 <https://link.springer.com/chapter/10.1007/978-3-030-51517-1_21> accessed 12 October 2021.

[250] ibid 253.

[251] Roy D'Souza and others, 'Publicly Verifiable Secret Sharing for Cloud-Based Key Management', *Progress in Cryptology – INDOCRYPT 2011* (Springer, Berlin, Heidelberg 2011) <https://link.springer.com/chapter/10.1007/978-3-642-25578-6_21> accessed 12 October 2021.

[252] Hanlin Zhang and others, 'Cloud Storage for Electronic Health Records Based on Secret Sharing with Verifiable Reconstruction Outsourcing' (2018) 6 IEEE Access 40713; Tatiana Ermakova and Benjamin Fabian, 'Secret Sharing for Health Data in Multi-Provider Clouds' [2013] Proceedings - 2013 IEEE International Conference on Business Informatics, IEEE CBI 2013 93.

On the other hand, it is true that *strong* encryption comes at a cost for fundamental rights. Law enforcement and intelligence services have always advocated for the creation of means (i.e., backdoors) that allow them to circumvent security solutions that cryptography provides[253]. To put a (temporary) halt to this quandary, the European Parliament, within discussions on ePrivacy Regulation amendments, proposed a set of constraints (on Member States attempts of breaking encryption) and facilitations (towards privacy and security of individuals' electronic communications), say, a *good infraethics*, in order "to safeguard the security and integrity of networks and services [and] to forbid Member States from imposing any obligation on encryption providers, providers of electronic communications services or any other organisations (at any level of the supply chain) that would result in the weakening of the security of their networks and services, such as the creation or facilitation of backdoors"[254].

In conclusion, by understanding *cybersecurity-as-a-good-infraethics* in the sole dimension of systems robustness, the powerful statement of Denardis can be seen in a more nuanced view:

> "*the need for strong cybersecurity is the common denominator of the most consequential public interest concerns of the present era. Privacy depends upon cybersecurity technologies. National security and the functioning of critical societal and industrial infrastructure require strong cybersecurity. Cybersecurity is increasingly connected to the legitimacy of democratic elections. Cybersecurity is necessary for human safety. Trust in financial systems and the stability of the global economic system depend upon cybersecurity"*[255].

Privacy and, more broadly, fundamental rights therefore depend upon *some* cybersecurity technologies, and not others. As it has been stressed above, by setting the right sort of infraethics i.e., the instrumental values we want to assign to security, the axiological state of affairs will accordingly be determined through balances, thus eschewing trade-offs. The following section attempts a closer investigation of the strand of cybersecurity as an infraethical facilitator of fundamental rights, namely system robustness, through the lens of the public goods doctrine.

---

[253] Koops and Kosta (n 137); Ziccardi, 'The GDPR and the LIBE Study on the Use of Hacking Tools by Law Enforcement Agencies' (n 137).

[254] European Parliament, Draft Report by Marju Lauristin (PE606.011v01-00), Respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Amendment 276, Sophia in 't Veld, Angelika Mlinar, Proposal for a regulation Recital 26 a (new).

[255] Denardis (n 17) 218.

2.2.3 Cybersecurity as a Public Good

An initial clarification on the legal-economical conceptual boundaries of "public goods" is advisable here. In economic theory, a good is 'public' when its consumption presents the characteristics of non-rivalry and non-excludability. In the first case, the good can be consumed by several agents simultaneously; in the second case, no member of society can be excluded from its consumption because exclusion would imply an excessive cost[256]. The latter, however, implies the possibility of using the good in question without bearing the costs: this phenomenon is called free riding.

A doctrine characterising cybersecurity as a public good is certainly not a theoretical novelty. For about twenty years, especially in the United States, several scholars have been developing theoretical models aimed at justifying the equation between cybersecurity and public goods, drawing analogies with national defence and with the protection of public health. Some have argued that only the objectives, and not the institutions, of public health – which is undisputedly a public good – can provide solid grounds for a rationale applicable by analogy to cybersecurity. Public health and cybersecurity both aim to achieve a positive outcome for society at large (health or security). This metaphor would mainly have two consequences. First, when balancing collective versus individual interests, the emphasis would be on the collective's. Second, the management of non-secure systems and networks would increasingly be handled by public intervention, through incentives and duties[257].

This theory combines three approaches: (i) persuasion through education, ideologies and social norms; (ii) monitoring through transparent information gathering and exchange; and (iii) state intervention in the choices of private individuals. Albeit intriguing and – to some extent – intuitive, this metaphor raises a number of theoretical and practical problems. The latter point (iii) in particular highlights the fact that if society wants to treat many, if not all, aspects of cybersecurity as a public good, then what the public health metaphor demonstrates is that it may be necessary to accept a higher level of coercion on behaviours than what hyper-historical[258] information societies are used to[259]. Moreover, a *tout court* application of the public good doctrine to the field of cybersecurity calls for a careful reflection on how to compensate for the underproduction of cybersecurity goods in a market failure scenario.

Section 2.1 has already pointed out that there is no stable consensus on the conceptual boundaries of "cybersecurity", both from a political and doctrinal standpoint. Yet, it is undisputed that cybersecurity does not consist of a single dimension, let alone a single product, capable of holistically addressing

---

[256] Patrick Mcnutt, 'Public Goods and Club Goods' (1999) 1 Encyclopedia of Law and Economics 927, 927.

[257] Deirdre K Mulligan and Fred B Schneider, 'Doctrine for Cybersecurity' (2011) 140 Daedalus 70.

[258] Luciano Floridi, *Il Verde e Il Blu - Idee Ingenue per Migliorare La Politica* (Raffaello Cortina Editore 2020) 85–91.

[259] Steven Weber, 'Coercion in Cybersecurity: What Public Health Models Reveal' (2017) 3 Journal of Cybersecurity 173 <https://academic.oup.com/cybersecurity/article/3/3/173/3836936> accessed 5 October 2021.

all the different cases of cyberthreats (viruses, malware, ransomware, DDoS, etc.). Rather, it is a mix of various assets, goods and processes. Many cybersecurity products and solutions, such as advanced cryptographic schemes, antivirus software, and intrusion detection systems[260], are not public goods: they are bought and sold between private sector actors, they are rivals, because their use affects other actors, and excludable, because their owners can restrict their use by others. Therefore, Rosenzweig argues that cybersecurity is a public good only and exclusively in its dimension of information-sharing regarding vulnerabilities and threats[261], since it is the only domain that is truly non-rival and non-excludable.

Similarly, a theory based on the classical tripartition of information security (see section 2.1) has been proposed. Taddeo argues that only the first domain – the robustness of the system, and therefore the degree of divergence between the current and the desired behaviour of the system – should be included in the public goods legal framework. Conversely, this doctrine would not be applicable to the remaining areas of cybersecurity, albeit for different reasons. In fact, as section 2.2.2 addressed above, resilience – understood in the dimension of threat detection – imposes a delicate balance between the desired degree of security and fundamental rights, such as the right to privacy and data protection; similarly, facilitating responsiveness may not lead to a global and collective improvement of cybersecurity. On the contrary, it is likely to lead to an intensification of cyberattacks[262].

The aim of this model is not to find an economic justification, but rather to lay the groundwork for a theoretical reflection on the need to treat the requirement of robustness of systems as a public good, due to the underlying public interest and crucial role it plays in tech-driven societies. Given the exponential growth of cyberattacks and threats, the non-rival but exclusive approach to this aspect of cybersecurity would continue to prove ineffective[263]. In general, developing robust systems has high costs: security aspects are often conceived in a trade-off with the final cost of the product. A case in point is the IoT sector, as seen in Chapter 1, where most of the connected devices are resource-constrained and for this reason more vulnerable to attacks.

A first direct consequence of applying the theory of public goods to cybersecurity would be to compare the externalities arising from the application of this doctrine.

---

[260] Christos Tselios, George Tsolis and Manos Athanatos, 'A Comprehensive Technical Survey of Contemporary Cybersecurity Products and Solutions' in Apostolos Fournaris and others (eds), *Computer Security LNCS11981 - ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC* (Springer, Cham 2019).

[261] Paul Rosenzweig, 'Cybersecurity and Public Goods The Public/Private "Partnership"' [2011] Emerging Threats in National Security and Law - Hoover Institution, Stanford University 7–9 <https://www.hoover.org/sites/default/files/research/docs/emergingthreats_rosenzweig.pdf> accessed 5 October 2021; N Eric Weiss, 'Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis' (2015) <https://sgp.fas.org/crs/misc/R43821.pdf> accessed 5 October 2021.

[262] Taddeo (n 225) 354.

[263] ibid 350.

The first negative externality to be analysed is the "diversionary effect": some cybersecurity technologies, such as firewalls, which arguably belong to the dimension of resilience, simply divert attacks from a more impenetrable target to one that is more easily attacked. This means that improving the security of one actor may lead to a lower security state for other systems[264], rather than increasing the overall level of security. In this context, circumscribing the public goods doctrine to the dimension of robustness alone, and not to cybersecurity *tout court*, would counter this externality, since the very rationale of this theoretical framework lies in the improvement of the overall level of cybersecurity.

A second negative externality is the "externalisation of costs": when software fails to prevent an intrusion or a service provider fails to block a malware attack, there is no mechanism by which these private actors can be held responsible for the costs of these failures. The costs are borne entirely by the end users[265]. The robustness of the system should not necessarily be free of charge for end users. On the other hand, it is essential that its costs do not become a discriminating factor, determining access: through a fair distribution of costs among the various market actors, access to appropriately secure digital technologies should be guaranteed for all users[266]. As a result, systemic, or holistic[267], approaches would be favoured i.e., focusing on the relationships between different cybersecurity technologies and, above all, on the outcome of these technologies in terms of their impact on the ecosystem in which they operate[268].

Managing system robustness as a public good also requires collaboration between the private and public sectors in order to ensure a high level of security, through a balanced division of competences and responsibilities. On the one hand, the public will have to establish standards, certification and testing, and supervision procedures, to ensure that a sufficient level of security is maintained to protect and promote the public interest, and that there are remediation and compensation measures when responsibilities are not properly discharged[269]. In this sense, Regulation EU 2019/881 (Cybersecurity Act) defines a European framework of cybersecurity certification schemes, to attest that ICT products, services and processes "comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the

---

[264] Rosenzweig (n 261) 9.

[265] ibid 10.

[266] Taddeo (n 225) 351.

[267] In the literature, the so-called "holistic approach" is gaining more and more support, although it has no single interpretation. Luciano Floridi and Andrew Strait, 'Ethical Foresight Analysis: What It Is and Why It Is Needed?' (2020) 30 Minds and Machines 77 <https://link.springer.com/article/10.1007/s11023-020-09521-y> accessed 5 October 2021; Charles D Raab, 'Information Privacy, Impact Assessment, and the Place of Ethics' (2020) 37 Computer Law & Security Review 105404; Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754.

[268] Taddeo (n 225) 350.

[269] ibid 351.

functions or services offered by, or accessible via, those products, services and processes throughout their life cycle"[270]. On the other hand, the private sector has a responsibility to design robust systems, develop and improve methods to foster the robustness of the services and products it offers, and cooperate with the public sector on controls and testing mechanisms[271].

In general, the need for structured public-private collaborations is evidenced by the growing number of initiatives and policy statements[272] emphasising the value of public-private partnerships (PPPs) to provide or enhance cybersecurity, especially in the field of critical infrastructure[273]. There are predominantly four areas of intersection, at a higher level of abstraction: (1) the reliable provision of access to the Internet and ICTs infrastructure; (2) the co-regulation of technical aspects of security and data processing; (3) the exchange of information on threats and vulnerability; and (4) mutual assistance in dealing with threats or illegal content in cyberspace[274].

Against this background of redistribution of responsibilities to all those who may be decisive in obtaining a satisfactory level of system robustness, with a view to protecting a common interest, some responsibilities will necessarily also fall on users, with particular reference to their "computer hygiene"[275]. In the words of Denardis, "[t]hose who purchase and install systems have a responsibility to be aware of the product's privacy and security policies, when available, including not only devices but also associated back-end systems and applications, and to take whatever precautions are available"[276].

From a legal point of view, such a conclusion would imply complex considerations on the desirability of different degrees of legal responsibility (e.g., contractual and extra-contractual liability) held by the users. From a comparative perspective, in the United States, in a workshop organised by NIST on

---

[270] Art. 46(2), Regulation EU 2019/881; Brunella Bruno, 'Cybersecurity Tra Legislazioni, Interessi Nazionali e Mercato' (2020) 14 Federalismi.it <https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=43404> accessed 5 October 2021.

[271] Taddeo (n 225) 351.

[272] Ministry of Foreign Affairs of Italy, 'Italian Position Paper on "International Law and Cyberspace"' (2021) 11 <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf>: "[I]taly considers public-private cooperation as key to guaranteeing cybersecurity and effective capacity-building".

[273] Luigi Martino and Francesco Cappelletti, 'Achieving Robust European Cybersecurity through Public-Private Partnerships: Approaches and Developments Content' (2021) 4 European Liberal Forum (ELF) <www.liberalforum.eu> accessed 5 October 2021; European Commission, 'Public Consultation on the Public-Private Partnership on Cybersecurity and Possible Accompanying Measures | Shaping Europe's Digital Future' (2015) <https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-public-private-partnership-cybersecurity-and-possible-accompanying-measures> accessed 5 October 2021; ENISA, 'Public Private Partnerships (PPP) - Cooperative Models ' (2018) <https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models> accessed 5 October 2021.

[274] Raphael Bossong and Ben Wagner, 'A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union' in Oldrich Bures and Helena Carrapico (eds), *Security Privatization: How Non-Security-Related Private Businesses Shape Security Governance* (Springer International Publishing 2018) 227.

[275] Taddeo (n 225) 352.

[276] Denardis (n 17) 120.

the cybersecurity of IoT devices, it emerged that the security of such systems should be a responsibility shared by producers and users[277]. Without dwelling too extensively on the liability issue here, which would go beyond the scope of this work, Article 122 of the Italian Consumer Code, in particular its second paragraph, may serve as an adequate legal basis for this responsibility framework[278].

In less controversial terms, computer "hygiene" could therefore consist of best practices that should become part of the skills of every Internet-user[279]. In the background of these reflections, however, remain the critical issues related to the digital divide[280], or *Onlife divide* - i.e., an exclusion not only from the mere dimension of connection, but from social life and knowledge[281] - although it has been shown that age is not always a vulnerability factor when it comes to perceiving the importance of such practices[282].

Such a recalibration of responsibilities, coupled with the need to consider the externalities arising from the production of cybersecurity goods, would facilitate cooperation between public and private actors and information-sharing on systems' vulnerabilities[283]. While the *public-private cooperation* is certainly the best interface on which we can better appreciate cybersecurity as a public good, due to its non-rival and non-exclusive nature[284], it may be wrong to assume that sharing information about vulnerabilities and threats generates a positive impact for all the stakeholders involved[285].

Firstly, software vulnerability is a sensitive issue that intersects the conflicting interests of cybersecurity (and, together, of privacy and personal data protection) and national security: law

---

[277] Katerina N Megas, Michael Fagan and David Lemire, 'Workshop Summary Report for "Building the Federal Profile for IoT Device Cybersecurity" Virtual Workshop NISTIR 8322' (2021) 9–10 <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8322.pdf> accessed 20 September 2021: : "eighty-two percent of responses to one poll question agreed that the responsibility for securing IoT devices is shared between manufacturer and customer. […] Customers, then, are responsible for implementing IoT devices in accordance with manufacturer guidance, ensuring devices have connectivity to receive updates, and monitoring devices to ensure continued security".

[278] Article 122(2), Codice del Consumo (D. Lgs. 6 September 2005, n. 206): *"[i]l risarcimento non è dovuto quando il danneggiato sia stato consapevole del difetto del prodotto e del pericolo che ne derivava e nondimeno vi si sia volontariamente esposto".*

[279] Lorenzo Pupillo, 'EU Cybersecurity and the Paradox of Progress ' (2018) 6–7 <https://www.ceps.eu/ceps-publications/eu-cybersecurity-and-paradox-progress/> accessed 5 October 2021.

[280] Ahmad Sultan, 'Improving Cybersecurity Awareness in Underserved Populations' [2019] CLTC White Paper Series Berkeley.

[281] Luciano Floridi and Massimo Sideri, 'Piramide Onlife' *Corriere Innovazione* (28 May 2021) 2.

[282] Scott M Schaffer, Daniel R Schaffer and Darlene G Colson, 'A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults ' (2020) 3 International Journal of Cybersecurity Intelligence & Cybercrime <https://www.doi.org/10.52306/03010420GXUV5876> accessed 5 October 2021.

[283] Taddeo (n 225) 352.

[284] Rosenzweig (n 261).

[285] Bossong and Wagner (n 274) 228.

enforcement and intelligence agencies, by exploiting so-called zero-days vulnerabilities[286], can more easily install malware in computer systems for law enforcement purposes[287], at the price of exposing the users of the system in question to attacks by malicious actors[288]. Therefore, it is easy to understand why Member States are reluctant to give up their prerogatives on vulnerability reporting[289].

Secondly, companies that are aware of cyber vulnerabilities, or that have been attacked[290], are reluctant to disclose them for fear of reputational consequences or possible liabilities for the event[291]. Indeed, the cost of disclosing an incident or threat is mainly private, as it is borne entirely by the company, while the benefits of better disclosure are pervasive. The imbalance between the costs borne by a company and the collective benefits generates a market failure.

On the one hand, this explains the temptation to move from the instrument of partnership to a more markedly top-down model of governance, consisting of institutionalised processes governing a "duty to notify"[292], albeit in contexts that guarantee confidentiality and reciprocity such as those identified in the computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs)[293]. On the other hand, it is clear that a new conceptual approach to cybersecurity is needed to make the behaviour of all market players more compatible with incentives[294]. The doctrine of the public good, in this sense, is an answer to this need.

In conclusion, the resulting theoretical framework is functional to outlining a model consisting of several proxies, or indicators, which can serve as a guide for the legal analysis of Chapter 3 on EU legal frameworks regulating (IoT) cybersecurity. At a high level of abstraction, the *redistribution of*

---

[286] A security flaw that is not yet known to the developers/producers of a computer system and, a fortiori, to the users of the system itself.

[287] Koops and Kosta (n 137) 898; Ziccardi, 'The GDPR and the LIBE Study on the Use of Hacking Tools by Law Enforcement Agencies' (n 137).

[288] Paul Stockton and Michele Golabek-Goldman, 'Curbing the Market for Cyber Weapons' (2015) 32 Yale Law & Policy Review 239 <https://digitalcommons.law.yale.edu/ylpr/vol32/iss1/11> accessed 5 October 2021.

[289] Stefano Fantin, 'Weighting the EU Cybersecurity Act: Progress or Missed Opportunity? ' (2019) <https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS2783850&context=L&vid=Lirias&search_scope=Lirias&tab=default_tab&lang=en_US&fromSitemap=1> accessed 5 October 2021.

[290] Of course, this would not apply to the subjects falling within the scope of the EU Directive 2016/1148 (NIS): operators of essential services must notify, without undue delay, the competent NIS authority (the CSIRT) of incidents with a "significant" impact on the services provided; providers of digital services must instead notify those incidents with a "substantial" impact.

[291] Gruppo di coordinamento sulla sicurezza cibernetica (GCSC) Banca d'Italia, 'Sicurezza Cibernetica: Il Contributo Della Banca d'Italia e Dell'Ivass ' (2018) 14 <https://www.bancaditalia.it/pubblicazioni/tematiche-istituzionali/2018-sicurezza-cibernetica/Tem_Istituzionali_sicurezza_cibernetica_agosto_2018.pdf> accessed 5 October 2021; Andrew Nolan, 'Cybersecurity and Information Sharing: Legal Challenges and Solutions' (2015) 5 <www.crs.gov> accessed 5 October 2021.

[292] Bossong and Wagner (n 274) 228.

[293] Banca d'Italia (n 291) 14–15.

[294] Pupillo (n 279) 7; Denardis (n 17) 117–118.

responsibilities, *cooperation* and *information-sharing* are cardinal elements for the doctrine of cybersecurity as a public good. Chapter 3 will assess whether and to what extent the newest legislative texts issued e.g., the NIS 2 Directive and the Cyber Resilience Act proposal, follow these indicators.

2.2.4 Degrees of separation between cybersecurity and safety in the IoT

The relationship between security and safety, which partly emerges in section 2.2.2, reflects a strand of the distinction between a condition of possibility for the enjoyment of instrumental goods (security-as-infraethics) and fundamental goods (security-as-a-fundamental-good, safety and fundamental rights). This section casts light on the distinction between the connected concepts of safety and security in a twofold manner: (i) the different understandings are interpreted in relation to the paradigm shift brought about by the IoT, which blends the physical and the virtual dimensions; (ii) how this distinction matters in relation to the relevant EU regulatory frameworks which form the subject matter of the next Chapter.

Reflections around safety and security have always been at the centre of the philosophical, political theory and legal debate – from Hobbes[295] and Locke[296] to Waltz[297], Bobbio[298] and Waldron[299]. According to the "pure safety conception", as Waldron put it, security is a function of individual safety. This make sense: we are more secure against cyberattacks when the probability of such a harmful event is reduced. Without entering Waldron's pure safety process of enrichment, in terms of breadth and depth, suffice here to say that this theory falls short of addressing collective and – more generally – "collateral" aspects that revolves around safety (e.g., fear, other types of harm rather than death or physical injury, assurance of being *actually* safe, etc.)[300].

Engaging in the flourishing scholarly debate on the relation between safety, security and trust, Durante acknowledges that whereas "[s]afety is mainly aimed to ensure the integrity of life against the threat of imminent dangers, [s]ecurity is mainly aimed to the protection of the conditions for the enjoyment of goods against the threat of dangers that may be subject of anticipation and calculation"[301]. A considerable divergence exists, according to the philosopher, in relation to the temporal sphere. Safety has a precise temporal dimension which is linked to *immediate* relationships,

---

[295] Thomas Hobbes, *Leviathan [1651]* (Richard Tuck ed, Cambridge University Press 1996).

[296] John Locke, *Two Treatises of Government [1690]* (Peter Laslett ed, Cambridge University Press 1967).

[297] Kenneth N Waltz, *Theory of International Politics* (Addison-Wesley Publishing Company 1979).

[298] Norberto Bobbio, *Future of Democracy* (Richard Dellamy and Roger Griffin (translated by) eds, Wiley Polity 1987).

[299] Jeremy J Waldron, 'Safety and Security' (2006) 85 Nebraska Law Review 455.

[300] ibid 461–463.

[301] Massimo Durante, 'Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks' in Don Berkich and Matteo Vincenzo D'Alfonso (eds), *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence*, vol 134 (Springer Nature 2019) 372.

whereas security has an inter-temporal nature which is grounded on *mediated* relationships. In this respect, the reflection revolves around security as "key policy lever" – due to the progressive conversion of security issues into safety issues (represented as more urgent and impending) – which allows governments to gain greater powers of direction and control with the aim of immunising society against the risks that seem to threaten its integrity[302].

Nevertheless, the "removal of a sphere of mediation between the request of fiduciary forms of risk management and their standardized and automated application"[303], which increasingly blurs the distinction between safety and security, is dealt with by the instruments of political theory. Although this critical reconstruction is useful for framing the boundaries of the concepts of safety and security, this section addresses this debate from a different angle.

What is at stake, here, is the harmonisation of legal philosophical, theoretical analyses of safety and security with the conceptualisation of technical literature, as this distinction plays a crucial normative role in shaping technologies, in particular, having regard to the IoT, through the means of standardisation[304].

Against this background, several authors argue that the paradigm shift brought by IoT, by bringing together the physical and cyber environment, increasingly leads to addressing traditional notions of security and safety in a more interchangeably or unified way[305], "in order to refer to different aspects of one and the same dimension as security flaws often turn out to be the flip-side of safety risks and vice versa"[306]. As a matter of fact, IoT health – referring here to "smart" pacemakers and insulin pumps, among others – is a prime example of how (cyber)security is increasingly taking on safety features, as security technologies and controls have to ensure the integrity of life against the threat of imminent dangers. Smart locks[307] and cars[308] are other clear cases where security threats, coming from the exploitation of flaws at design and implementation level, might jeopardize individual safety. Moreover, attacks on national critical infrastructure – from hospitals and water supplies to banks,

---

[302] ibid 379.

[303] ibid.

[304] Anton Vedder, 'Safety, Security and Ethics' in Anton Vedder and others (eds), *Security and Law* (Intersentia 2019) 11.

[305] Marilyn Wolf and Dimitrios Serpanos, *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems* (Springer 2020) 35–36.

[306] Vedder (n 304) 21.

[307] Grant Ho Derek Leung Pratyush Mishra Ashkan Hosseini Dawn Song David Wagner and others, 'Smart Locks: Lessons for Securing Commodity Internet of Things Devices' (2016) <http://www.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-11.html> accessed 14 October 2021.

[308] Mike Spector and Danny Yadron, 'Regulators Investigating Fiat Chrysler Cybersecurity Recall ' *The Wall Street Journal* (24 July 2015) <https://www.wsj.com/articles/fiat-chrysler-recalls-1-4-million-vehicles-amid-hacking-concerns-1437751526> accessed 14 October 2021.

police departments and transportation – reveal the true magnitude of IoT cyberthreats. Countless injuries, or even deaths, may incur as a result thereof. In late 2021, the Secretary of US Department of Homeland Security Alejandro Mayorkas referred to these new menaces as *killware*[309].

Among others, Serpanos and Wolf present a unified safety and security design methodology based on a holistic threat analysis. The authors initially build the distinction between safety and security according to different level of abstractions within the threat analysis paradigm: whereas safety threats analysis start from the risks linked to the *application domain*, security assessments focus prominently on *systems' architecture* and *module design*[310]. They further distinguish security from safety properties. The former conceives information in an all-or-nothing fashion; the latter emphasises operation with reduced capability as safety attacks may be limited to certain time window[311]. It therefore appears necessary to recall the above-mentioned temporal and intertemporal connotations associated with safety and security. Albeit within a holistic understanding, they acknowledge that such concepts respectively operate at different technical implementation levels.

Traditionally, IT literature considers physical safety as the result of the absence or minimisation of hazards that may harm both life and property; computer security used to focus on the CIA triad, as addressed in section 2.1. Can safety, therefore, be considered as a requisite of cybersecurity? Hildebrandt, thus, points out that *traditional* digital security, that is, computer security, does not necessarily involve safety, providing an example in which a cyberattack towards a web platform does not jeopardise anybody's safety[312].

Yet, the hyper-connectedness of *every* social sphere brought by the IoT shows the dependence of "human safety on encryption, authentication, data integrity, availability, and other dimensions of cybersecurity"[313]. In this regard, increased cybersecurity – in its dimension of robustness – *does* imply increased individual safety. And the contrary seems to be no longer true[314]. With the advent of the IoT, safety has become a requirement for cybersecurity, which has the ability to (re-)shape systems' architecture and design, therefore directly influencing safety properties.

---

[309] Josh Meyer, 'The next Big Cyberthreat Isn't Ransomware. It's Killware. And It's Just as Bad as It Sounds' *USA Today* (12 October 2021) <https://eu.usatoday.com/story/news/politics/2021/10/12/cybersecurity-experts-warn-killware-attacks-rival-ransomware/6042745001/> accessed 18 October 2021.

[310] Wolf and Serpanos (n 305) 35–36.

[311] ibid 35.

[312] Hildebrandt (n 183) 260.

[313] Denardis (n 17) 184.

[314] Hildebrandt (n 183) 260.

At the same time, safety requirements include infrastructure (cyber)security ones: "security is a requirement for safety as well, since data integrity is necessary at least"[315]. A similar reasoning can be found in the European Commission Communication on "Building Trust in Human-Centric Artificial Intelligence", according to which emerging digital technologies "should integrate safety and security-by-design mechanisms to ensure that they are verifiably safe at every step, taking at heart the physical and mental safety of all concerned"[316].

All in all, in the IoT era, safety, cybersecurity and privacy can no longer be deemed as separate domains. Instead, they will increasingly interact and affect each other. Therefore, *holistic* approaches[317] for the assessment of 'security & privacy' risks in the IoT will be required. In this respect, Chapter 5 specifically integrates security requirements in a data protection model (data protection impact assessment i.e., DPIA).

A normative distinction between the concepts of safety and security matters vis-à-vis the legal frameworks that regulate each aspect in the IoT context. As addressed in the next chapter, in the EU, product safety legislation aims to ensure the public policy objective of placing products in the single market that meet high health, safety and environmental requirements and that such products can circulate freely throughout the Union. Safety is usually conceived in a broad context, defined in "the code of ethical conduct of robotics engineers" – in the European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics – as *physical wellbeing, safety, health and rights*[318].

Moreover, the concept of safety is linked to the use of the product and the risks – including also cyber risks and risks related to the loss of connectivity of devices – to be addressed to make the product safe[319]. The EU Commission acknowledges that connectivity challenges the traditional understanding

---

[315] Dimitrios Serpanos and Marilyn Wolf, *Internet-of-Things (IoT) Systems - Architectures, Algorithms, Methodologies* (Springer International Publishing 2018) 57.

[316] European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Building Trust in Human-Centric Artificial Intelligence COM/2019/168 Final' (2019) 5 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52019DC0168> accessed 12 October 2021.

[317] Andrew J Grotto and Martin Schallbruch, 'Cybersecurity and the Risk Governance Triangle' (2021) 2 International Cybersecurity Law Review 77 <https://link.springer.com/article/10.1365/s43439-021-00016-9> accessed 4 November 2021.

[318] European Parliament, 'European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))' (2017) 20 <https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf> accessed 18 October 2021.

[319] European Commission, 'REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics COM/2020/64 Final' (2020) 6 <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064> accessed 12 October 2021.

of safety, as it may compromise the safety of the product, and indirectly when it can be hacked leading to security threats and affecting the safety of users[320].

Besides Directive 95/2001/EU (General Product Safety Directive, hereinafter GPSD), which applies to all product categories as *lex generalis* (usually referred to in as "safety net"), the siloed thinking underpinning the rationale of the New Legislative Framework (NLF)[321] results in a sectoral regulatory approach. Therefore, the application of safety essential requirements to IoT devices depends on their classification according to product categories[322]. As addressed in Chapter 3, these Regulations and Directives were enacted before IoT hyper-connection. As a result, they risk being outdated when facing new cybersecurity threats that may result in safety harms[323].

2.3 Conclusion

Security, safety, privacy and data protection are ever more intertwined in the age of IoT: a normative, theoretical reflection on the distinct underlying rationales and scopes of these values is therefore needed to orient the legal analysis of the EU legal frameworks that regulate those aspects in the following chapters.

Cybersecurity has not merely replaced the 'old fashioned' technical concepts of computer and information security. This chapter showed that it represents a new paradigm. Limiting the concept of 'security' in the cyber domain to the protection of networks, information systems and information is too restrictive and ultimately anachronistic. The IoT era expands the *perimeter* of the values and assets that need to be protected. Risk factors and threats in today's IoT hyper-connected digital

---

[320] ibid 5.

[321] The new legislative framework (NLF) aims to improve the internal market for goods and strengthens the conditions for placing a wide range of products on the market (CE marking), *via* a package of measures which improves market surveillance and boosts the quality of conformity assessments. The NLF consists of (i) Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products; (ii) Decision 768/2008 on a common framework for the marketing of products, which includes reference provisions to be incorporated whenever product legislation is revised; and (iii) Regulation (EU) 2019/1020 on market surveillance and compliance of products.

[322] The directives and regulations that Decision 768/2008/EC aligned with, or was based on, the principles of NLF reference provisions are: Toy Safety - Directive 2009/48/EU; Transportable pressure equipment - Directive 2010/35/EU; Restriction of Hazardous Substances in Electrical and Electronic Equipment - Directive 2011/65/EU; Construction products - Regulation (EU) No 305/2011; Pyrotechnic Articles - Directive 2013/29/EU; Recreational craft and personal watercraft - Directive 2013/53/EU; Civil Explosives - Directive 2014/28/EU; Simple Pressure Vessels - Directive 2014/29/EU; Electromagnetic Compatibility - Directive 2014/30/EU; Non-automatic Weighing Instruments - Directive 2014/31/EU; Measuring Instruments - Directive 2014/32/EU; Lifts - Directive 2014/33/EU; ATEX - Directive 2014/34/EU; Radio equipment - Directive 2014/53/EU; Low Voltage - Directive 2014/35/EU; Pressure equipment - Directive 2014/68/EU; Marine Equipment - Directive 2014/90/EU; Cableway installations - Regulation (EU) 2016/424; Personal protective equipment - Regulation (EU) 2016/425; Gas appliances - Regulation (EU) 2016/426; Medical devices - Regulation (EU) 2017/745; In vitro diagnostic medical devices - Regulation (EU) 2017/746; EU fertilising products – Regulation (EU) 2019/1009.

[323] Eduard Fosch-Villaronga and Tobias Mahler, 'Cybersecurity, Safety and Robots: Strengthening the Link between Cybersecurity and Safety in the Context of Care Robots' (2021) 41 Computer Law & Security Review 6.

environment go beyond the technological infrastructure of information systems, networks and the underlying information. An attack could also infringe individuals' fundamental rights, impair physical safety and, as much as the critical infrastructure is concerned, have serious consequences for communities, institutions and businesses.

As regards the relationship between cybersecurity and the fundamental right to privacy (understood within the theory of informational privacy, to include personal data protection issues), the chapter has explored two possible perspectives. Cybersecurity as an *instrumental* value to uphold *fundamental* values (e.g., fundamental rights and liberties, physical safety) and cybersecurity as a *fundamental* value *per se,* involving therefore balancing exercises in the event of compression of other fundamental values on the same level. Building on the three dimensions of cybersecurity (i.e., robustness, resilience and response), the analysis concludes that only in the latter two cases does cybersecurity pose risks to privacy. In this respect, bad '*infraethics*' apply trade-offs rather than balances. Privacy is therefore 'facilitated' by *some* cybersecurity technologies and not others.

On the contrary, the first dimension of cybersecurity i.e., systems' robustness, which focuses on building solid, reliable systems that can withstand and mitigate attacks, shall be seen within the *instrumental* or *infraethical* horizon. Yet, an attempt has been made in developing a theoretical framework for the application of the public good theory to this sole dimension of cybersecurity, developing the model of Taddeo. Without neglecting the possible externalities that may arise, the resulting model pivots around three pillars, which can be observed in the recent EU legislative developments in EU cybersecurity *acquis*, as addressed in Chapter 3. These are: redistribution of responsibilities, cooperation between private and public sectors and information-sharing.

Finally, the chapter shed light on the distinction between the concepts of (cyber)security and safety. The IoT paradigm shift, which brings together the physical and cyber environment, increasingly leads to the addressing of traditional notions of security and safety in a more holistic way. With the advent of the IoT, increased cybersecurity *does* imply increased individual safety. Safety becomes a requirement for cybersecurity, which has the ability to (re-)shape systems' architecture and design, directly influencing safety properties. This reflection would serve as a solid benchmark in critically analysing the EU legal frameworks regulating IoT security & safety in Chapter 3.

Chapter 3. The EU Legal Frameworks Regulating IoT Cybersecurity

3.1 Cybersecurity in the EU: a Brief Historical Background

The evolution of the concept of cybersecurity, as addressed in Chapter 2, is echoed in the actions of the EU legislator. Initially, security was geared towards ensuring the functioning of public communications networks: in the Council Directive 90/387/CEE, security of network operations was an essential requirement that could be the grounds for the Member States' power to restrict access to the public telecommunications network or public telecommunications services[324]. The necessity of protecting communication networks led to the adoption of regulatory safeguards in Directives on data protection[325] and in the legal framework for telecommunications services[326], in order to ensure a minimum level of security.

By proposing a European policy approach on NIS in 2001, the Commission's Communication on Network and Information Security[327] marked a watershed in European "digital" security law[328]. The

[324] Council Directive of 28 June 1990 on the establishment of the internal market for telecommunications services through the implementation of open network provision (90/ 387/EEC), Article 2(6); Article 3(2).

[325] Directives 95/46/EC (OJ L281 of 23.11.1995) and 97/66/EC (OJ L24 of 30.1.1998)

[326] Commission Liberalisation Directive 90/388/EC, Interconnection Directive 97/33/EC, Voice Telephony Directive 98/10/EC.

[327] European Commission, 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions Network and Information Security: Proposal for A European Policy Approach' (2001) 3 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298>. For the first time, the Commission defines network and information security as "the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions. Such events or actions could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems".

[328] European Commission, 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions Network and Information Security: Proposal for A European Policy Approach' (n 327).

rationale behind this policy initiative was to provide the missing link in a regulatory framework where data protection & telecom, cybercrime[329] and NIS would be interrelated[330].

Then, in 2004, the European Network and Information Security Agency (ENISA) was established, initially for a period of five years[331], to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union[332]. The Agency was tasked, *inter alia,* with collecting appropriate information to analyse current and emerging risks, providing EU institutions and competent national bodies with advice and enhancing cooperation between different actors operating in the field of network and information security[333]. Building on the 2005 EC Communication on the need to coordinate efforts to build trust and confidence of stakeholders in electronic communications and services[334], in 2006 the Commission, in order to tackle the challenges of network and information security – including, but not limited to attacks, usage of mobile devices, the advent of ambient intelligence and the raising of user awareness – proposed an approach based on dialogue, partnership and empowerment[335]. Eventually, Council Resolution 2007/068/01 endorsed the key points of the 2006 EC strategy.

In parallel to the European Programme for Critical Infrastructure Protection (EPCIP)[336], which prepared the ground for Directive 2008/114/EC[337], the Commission proposed an integrated EU multi-stakeholder and multi-level approach to enhance the security and resilience of the Critical Information

---

[329] EU rules on cybercrime correspond to and build on different provisions of the 2001 Council of Europe Convention on Cybercrime (Treaty No. 185, also known as the Budapest Convention), which was considered by the European Council "the legal framework of reference for fighting cyber-crime at global level", European Council, ' The Stockholm Programme - An Open and Secure Europe Serving and Protecting Citizens' (2010) 22 <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF> accessed 23 November 2021.

[330] European Commission, 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions Network and Information Security: Proposal for A European Policy Approach' (n 327) 19–20.

[331] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, article 27. Regulation (EC) No 1007/2008 then extended the mandate until March 2012.

[332] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, article 1(1).

[333] ibid article 3.

[334] European Commission, 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "I2010-A European Information Society for Growth and Employment" COM(2005) 229 Final' (2005).

[335] European Commission, 'Communication from the Commission of 31 May 2006: A Strategy for a Secure Information Society "Dialogue, Partnership and Empowerment" COM(2006) 251 final' (2006) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al24153a>.

[336] European Commission, 'Communication from the Commission on a European Programme for Critical Infrastructure Protection' (2006) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN> accessed 24 November 2021.

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

Infrastructure (CII)[338], in the face of rising disruptions and cyber-attacks[339]. The objective of enhancing the security and resilience of CIIs led to reform the regulatory framework for electronic communications networks and services[340] with new provisions in terms of security and integrity, including *inter alia* obligations for providers of public communications networks or publicly available electronic communications services to implement technical and organisational measures to appropriately manage the risks posed to the security of networks and services and to notify of any security breach (Article 13a). "This step-change was a significant move away from a voluntary approach (which characterised the 2006 communication, for example), with ENISA tasked in supporting member states to implement Article 13a through establishing a standard incident reporting methodology and mechanism"[341].

In 2010, the Commission put forward the Digital Agenda for Europe *with the overall objective of delivering sustainable economic and social benefits from a digital single market based on fast and ultra-fast internet and interoperable applications*. With regards to security, the Commission announced measures aiming at a reinforced and high-level Network and Information Security Policy, including legislative initiatives such as a modernised European Network and Information Security Agency (ENISA), and measures – including legislative initiatives – allowing faster reactions in the event of cyber-attacks against information systems (such as a CERT for the EU institutions)[342]. Six months later, the Internal Security Strategy further addressed major issues related to cybercrime,

---

[338] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from Large Scale Cyber-Attacks And ' (2009) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF> accessed 24 November 2021. Accordingly, the Communication focuses on five pillars: (1) Preparedness and prevention: to ensure preparedness at all levels; (2) Detection and response: to provide adequate early warning mechanisms; (3) Mitigation and recovery: to reinforce EU defence mechanisms for CII; (4) International cooperation: to promote EU priorities internationally; (5) Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures.

[339] George Christou, 'Introduction', *Cybersecurity in the European Union* (Palgrave Macmillan UK 2016) 1.

[340] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

[341] George Christou, 'Network and Information Security and Cyber Defence in the European Union', *Cybersecurity in the European Union* (Palgrave Macmillan UK 2016) 124.

[342] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe COM(2010) 245 Final' (2010) 16–19 <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> accessed 24 November 2021.

cybersecurity and privacy addressed by the Digital Agenda as the main components in building trust and security for network users[343].

Against this background, in 2013 the Commission adopted the first, comprehensive, Cybersecurity Strategy, outlining the EU's vision in this domain, clarifying roles and responsibilities and setting out the actions required based on the strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world[344]. For the first time, the term *cybersecurity* entered the official lexicon of EU institutions. Thus, a footnote in the introduction specifies that cybersecurity

> *"[c]ommonly refers to 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"*[345].

Whereas the first part of the definition tends to be more all-encompassing with regard to the scope of protection of cybersecurity, the second phrase partially narrows it down to the upholding of the so-called CIA (i.e., confidentiality, availability and integrity) triad, the cornerstone of computer and information security. This notwithstanding, the broad set of principles that ought to guide EU cybersecurity policy demonstrates the intention to stretch the boundaries of this domain[346]. Not surprisingly, later on in the Strategy, emphasis is placed on the relationship with fundamental rights and freedoms as enshrined in the CFR of the EU, echoing the *infraethical* perspective stressed in Chapter 2: on the one hand, cybersecurity "can only be sound and effective if it is based on EU core values"; on the other, "individuals' rights cannot be secured without safe networks and systems"[347]. To conclude, the vagueness of the definition of such a broad and evolving term leaves room for the

---

[343] European Commission, 'Communication from the Commission to the European Parliament and the Council The EU Internal Security Strategy in Action: Five Steps towards a More Secure Europe COM(2010) 673 Final' (2010) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF> accessed 24 November 2021.

[344] European Commission, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 Final' (2013) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN> accessed 24 November 2021.

[345] ibid 3.

[346] ibid 3–4.

[347] ibid 4.

stakeholders and policy makers to consider which 'contextual definition' best suits their requirements[348].

The Strategy articulates five strategic priorities: (i) achieving cyber resilience; (ii) drastically reducing cybercrime; (iii) developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP); (iv) developing the industrial and technological resources for cybersecurity; (v) establishing a coherent international cyberspace policy for the European Union and promoting core EU values. As regards the first area of action, consistently with the paradigm shift vis-à-vis the EU governance of cybersecurity, namely "from hands-off meta-governance to a more hands-on mandatory stance"[349], the Commission invited the European Parliament and the Council to adopt the proposal for a "Directive on a common high level of Network and Information Security (NIS) across the Union". This legal act was seen as a means to address Member States' cybersecurity capabilities and preparedness, EU-level cooperation and take up of risk management practices, reporting of major cyber incidents and information sharing on NIS[350]. In parallel, Regulation (EU) 526/2013 was adopted to strengthen and modernise ENISA, albeit the mandate remained temporarily[351].

Lastly, while recalling that all parties – whether public authorities, the private sector or individual citizens – "need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity"[352], the Commission acknowledges that "a key challenge is to clarify the roles and responsibilities of the many actors involved"[353]. Therefore, to address cybersecurity in a comprehensive fashion, the multi-stakeholder and multi-level model was designed to span across three key pillars — NIS, law enforcement, and defence — operating within different legal frameworks that would involve both national governments and the EU.

---

[348] ENISA, 'Definition of Cybersecurity: Gaps and Overlaps in Standardisation' (2015) 28; Fuster and Jasmontaite (n 180) 103.

[349] Christou (n 341) 132.

[350] European Commission, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 Final' (n 344) 5–7.

[351] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004. Article 36 established the duration of the Agency for a period of seven years from 19 June 2013.

[352] European Commission, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 Final' (n 344) 4.

[353] ibid 17.

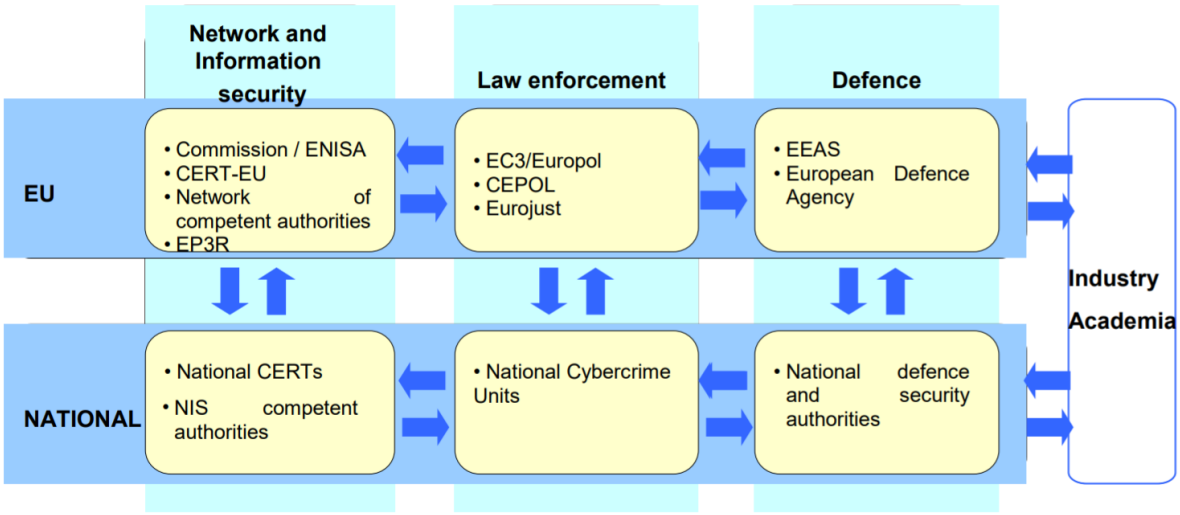


Figure 2: The multi-stakeholder and multi-level model of governance of EU Cybersecurity designed by the 2013 Cybersecurity Strategy[354]

While the NIS Directive (Directive EU 2016/1148) will be further scrutinised from a legal perspective in the following section, the remaining sections of the chapter will account for the latest development (that is, from 2016 onwards) of the EU governance approach in the field of (IoT) cybersecurity.

3.2 Security of Network and Information (IoT) Systems

3.2.1 The NIS Directive and the indirect link with the IoT

The more they play a vital role in our society, the more network and information systems and services are at risk. Their reliability and security are both crucial aspects for upholding the functioning of the market as well as for the protection of the rights and liberties of individuals. Against this backdrop, Directive (EU) 2016/1148 (hereinafter, the Directive)[355] is the first piece of EU-wide legislation on cybersecurity, providing legal measures to boost the overall level of cybersecurity in the Union.

The Directive lays down measures with a view to achieving a high common level of security of network and information systems (NIS) within the Union – conceived as a baseline set of *minimum* cybersecurity standards, establishing a *lex generalis – lex specialis* relationships with already existing or future EU sector-specific legislation with NIS-related rules[356] that will be addressed in the next

[354] ibid.

[355] 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.

[356] Directive (EU) 2016/1148, article 1(7); recital 9.

section – in order to improve the functioning of the internal market[357], therefore having as legal basis Article 114(1) of the Treaty on the Functioning of the European Union (TFEU)[358]. Accordingly, the resulting responsibility to ensure NIS security mostly lies – besides Member States[359] – with the two macro categories of actors under the scope of the Directive: operators of essential services (OES) and digital service providers (DSP).

In particular, the onus of identifying the OESs is placed on Member States which, pursuant to Article 5 of the Directive, shall determine which entities, having an establishment on their territory, ought to be classified as OESs. These entities are to be sought in those actors whose services' provision depends on network and information systems[360] throughout seven pre-identified sectors[361] – and relative subsectors – deemed as essential for the maintenance of critical societal and economic activities[362]. The significant disruptive effects that an incident would have on the provision of the service is yet a further criterion for the identification of OESs[363]. To weigh the significance of a "disruptive effective", Member States shall take into account not only several *cross-sectorial factors* – such as the number of users affected, the degree and duration of the impact on economic and societal activities or public safety, the geographic spread, the market share of that entity, the dependency of other sectors on the service provided by that entity, and the importance of the entity for maintaining a sufficient level of the service[364] - but *sector specific factors* as well[365]. Interestingly, the Directive may not apply indiscriminately to every public administration, but only to those that are identified as

[357] Directive (EU) 2016/1148, article 1(1).

[358] Consolidated version of the Treaty on the Functioning of the European Union *OJ C 326, 26.10.2012*, article 114(1): [T]he European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

[359] Within Member states obligations, Article 7 mandates the adoption of a national NIS/cybersecurity strategy, defining the strategic objectives and appropriate policy and regulatory measures; Article 8 imposes on each Member State the duty to designate one or more national competent authorities on the security of NIS and a single point of contact; whereas Article 9 foresees the obligation to designate one or more CSIRTs (which could be established within a competent authority).

[360] Directive (EU) 2016/1148, Article 5(2)(b).

[361] Directive (EU) 2016/1148, Annex II: (i) energy; (ii) transport; (iii) banking; (iv) financial market infrastructures; (v) health sector; (vi) drinking water supply and distribution; (vii) digital infrastructure.

[362] Directive (EU) 2016/1148, Article 5(2)(a); Recital 20.

[363] Directive (EU) 2016/1148, Article 5(2)(c).

[364] Directive (EU) 2016/1148, Article 6(1).

[365] Directive (EU) 2016/1148, Article 6(2), Recital 28: for example, with regard to energy suppliers, "such factors could include the volume or proportion of national power generated".

OESs[366]. Finally, in those cases where an OES offer its services in two or more Member states, those States shall engage in bilateral/multilateral consultations[367].

Conversely, the threefold classification of DSP, i.e., online marketplaces, online search engines and cloud computer services[368], covers every entity falling into one of those categories. Hence, Member States do not have to identify them. The ratio of this divergence of treatment has to be found in the almost unavoidable reliance on DSPs services by EU businesses and users, including OESs[369]. Moreover, the Directive considered OESs and DSPs *fundamentally* different in that the former have a direct link with physical infrastructure while the latter have a cross-border nature[370]. Hence, the EU legislator wanted to eschew a scenario of a lack of harmonisation vis-à-vis the identification – with the subsequent application of NIS obligations in terms of security measures and incidents reporting – of DSPs by Member States.

The differentiation in treatment of OESs and DSPs does not amount solely to their identification by Member States. As regards security and incidents notification requirements for OESs and DSPs, arguably the core of the Directive, in Chapter IV and V respectively, the Directive lays down stricter obligations for operators of essential services than the ones foreseen for digital service providers. The rationale behind this approach was the assumption that the degree of risk for operators of essential services is higher than for digital service providers, resulting in lighter security requirements for digital service providers[371]. As a result, Member States are not allowed to impose any further security or incidents notification requirements on DSPs, other than the ones laid down at Article 16[372]. The nature of DSPs' operations justified the so-called "light-touch"[373], which is prominent in the implementation and enforcement phase. Thus, Member States' competent authorities can only take action on DSPs through *ex-post* supervisory measures, when provided with evidence that a digital service provider does not meet the security and incidents notification requirements[374]. The difference with the corresponding Article 15 is striking: in particular, competent authorities shall have the powers and means to require – at any time – OESs to provide the information necessary to assess the

[366] Directive (EU) 2016/1148, recital 45.
[367] Directive (EU) 2016/1148, article 5().
[368] Directive (EU) 2016/1148, Annex III.
[369] Directive (EU) 2016/1148, recital 48.
[370] Directive (EU) 2016/1148, recital 57.
[371] Directive (EU) 2016/1148, recital 49.
[372] Directive (EU) 2016/1148, article 16(10).
[373] Directive (EU) 2016/1148, recital 60.
[374] Directive (EU) 2016/1148, article 17(1).

security of their NIS and evidence of the effective implementation of security policies (e.g., results of a security audit)[375].

This lighter regime has received a lot of criticism in literature, given the crucial importance of DSPs (for example, we can refer to ubiquitous cloud service providers) in today's society and economy[376]. There is an unavoidable dependency of our societies on DSPs that is acknowledged by the Directive itself[377]. However, ENISA helps in clarifying that "applying a light touch approach should not prevent a specific authority from being fully able to exercise its supervision authority upon a DSP, should the case require it. For example, applying fewer provisions for DSPs as compared to OES might not be beneficial if certain limits are exceeded"[378]. Moreover, the possibility of public administrations to require DSPs to have additional security measures, for the services they use, *via* contractual obligations can be seen as a partial mitigation of the light-touch approach[379].

As regards the security and incident notifications requirements, Article 14(1) does not give any indication on the nature, appropriateness, and proportionality of technical and organisational measures that OES shall take in managing the risks (involving therefore measures to prevent and minimise the impact of incidents[380]) posed to the security of network and information systems. Rather, security measures and controls are ultimately decided by the OES, following a risk-based approach, as the European legislator opted for a principles-based model of governance, rather than enforcing prescriptive rules[381]. Notwithstanding the security measures put in place by the OES, if an incident – with a *significant* impact (in terms of the numbers of users affected, the duration and the geographical spread) on the continuity of the essential services provided – occurs, the OES must notify the competent authority or CSIRT[382] without undue delay[383].

---

[375] Directive (EU) 2016/1148, Article 15(2).

[376] Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation' (2019) 35 Computer Law and Security Review 105336 <https://doi.org/10.1016/j.clsr.2019.06.007>.

[377] Directive (EU) 2016/1148, Recital 48.

[378] ENISA, 'Incident Notification for DSPs in the Context of the NIS Directive - A Comprehensive Guideline on How to Implement Incident Notification for Digital Service Providers, in the Context of the NIS Directive' (2017) 9–10.

[379] Directive (EU) 2016/1148, Recital 54.

[380] Directive (EU) 2016/1148, Art. 14(2).

[381] Mark D Cole and Sandra Schmitz, 'The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape' (2020) 017 8: "[w]hile the national transposition of the NIS Directive repeat the general wording of the Directive, complementary guidance or regulations amending national law define the indefinite legal concepts further".

[382] Directive (EU) 2016/1148, Art. 14(5): "the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State".

[383] Directive (EU) 2016/1148, Arts. 14(3), 14(4).

Albeit following the same risk-based approach[384], Article 16 includes specific elements that DSPs have to take into account when identifying the security measures. These are: (a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing and testing; (e) compliance with international standards[385]. This specification, absent in the corresponding Article 14, can be attributed to the aforementioned "light-touch": given the softer control and enforcement, the Directive wants to make sure that at least baseline requirements are met. Like OESs, DSPs must notify the competent authority or CSIRT[386], without undue delay, of any incident having a *substantial* impact on the services provided[387]. The three parameters that apply for determining the significance of the impact of an incident affecting an OES are added to by two more: (i) the extent of the disruption; and (ii) the extent of the impact on economic and societal activities[388]. Interestingly, if an OES relies on a service provided by a DSP, which is essential for the maintenance of critical societal and economic activities, and yet an incident affects the DSP, the OES has to notify the NIS authority of the event if it results in a *significant* impact on the continuity of the essential services, leaving the DSP off the hook. However, where an incident has a *substantial* impact on the provision of a digital service, but the impact on the continuity of an OES is not significant, the DSP will have to notify.

[384] Directive (EU) 2016/1148, Art. 16(2): "Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems".

[385] Directive (EU) 2016/1148, Art. 16(1). These elements were further specified by the Commission Implementing Regulation (EU) 2018/151, in article 2.

[386] Directive (EU) 2016/1148, Art. 16(6): "[i]f the incident […] concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States".

[387] Directive (EU) 2016/1148, Art. 16(3).

[388] Directive (EU) 2016/1148, Art. 16(4).

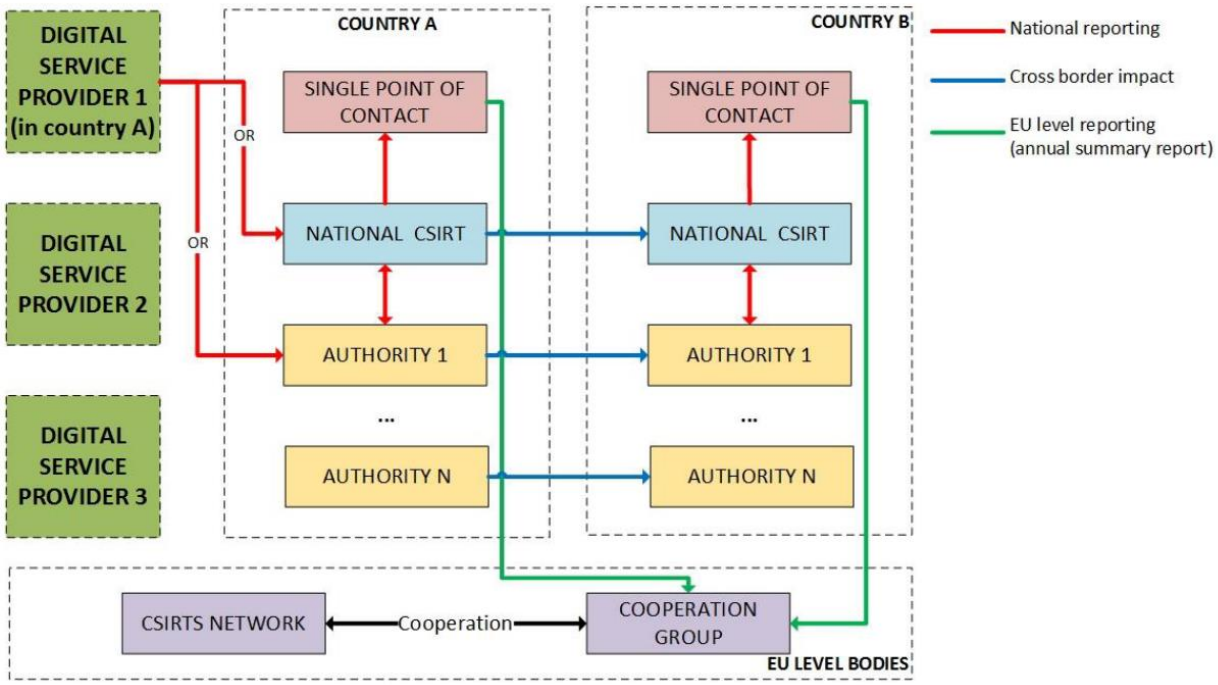


Figure 3: DSPs incident notification process in the NIS Directive[389]

Against the background of the NIS Directive's scope, the question arises as to whether and to what extent the Directive addresses IoT security challenges. First, a link between the IoT and the Directive has to be established. This section has clearly shown that the NIS Directive was not conceived to *directly* enhance products' cybersecurity or were the terms "Internet of Things" or "new emerging technologies" mentioned in the legislative act. Yet, Article 4(1)(b) of the Directive defines "network and information systems" as "any device or group of interconnected or related devices, one or more of which, pursuant to a programme, perform automatic processing of digital data"[390]. As long as these devices are connected to the Internet, this provision arguably includes IoT systems in the scope of the Directive. It follows that if an OES or a DSP, in the context of the provision of their services (that must be essential to societal and economic activities, as regards OES), relies on the deployment of an IoT system, it *must* take the appropriate and proportionate technical and organisational cybersecurity measures and controls to manage the risks – following the risk-based approach – posed to that particular IoT system or device.

Although the NIS Directive enhanced the overall level of cybersecurity in the Union, critical issues have been raised regarding the standard of protection it enforced. In particular, given its peculiar

[389] ENISA, 'Incident Notification for DSPs in the Context of the NIS Directive - A Comprehensive Guideline on How to Implement Incident Notification for Digital Service Providers, in the Context of the NIS Directive' (n 378) 18.

[390] Directive (EU) 2016/1148, Art. 4(1)(b).

architecture, with regard to IoT – as presented in Chapter 1, the challenges posed by the differentiation in treatment of OESs and DSPs mentioned above (the "light-touch") are particularly evident. Let us think of the case of an OES that provides its essential service through the adoption of IoT systems. For example, a supplier or distributor of drinking water deploys connected sensors that monitor quality levels and actuators that manage the quantity levels of chemicals in the water, to help to maintain the pH stability. Now, almost any IoT device resorts to the cloud for data storage and processing. It follows that a DSP is involved to the extent that it provides cloud computing resources and services to such IoT systems.

This brings three main consequences. First, the overall security of an OES relying on IoT systems will ultimately also depend on the adequacy – in terms of both appropriateness and proportionality – of the technical and organisational cybersecurity measures implemented by the DSP. Nevertheless, the light enforcement granted by the Directive to DSPs, through eventual and *ex post* supervisory measures issued by national competent authorities[391], might jeopardise the correct provision of services that are essential to societal and economic activities. Second, if an incident, occurring at cloud level, does not meet the quantitative and qualitative thresholds established by the Implementing Regulation (EU) 2018/151[392], and thus it could not be deemed *substantial* but, at the same time, it has *significant* impact on the continuity of the essential services provided by the OES, then it is the OES that has to notify the event to the NIS authority. In cybersecurity, incident handling procedures and timeframes are crucial[393]. The more time an OES spends on comprehensively understanding the extent of the incident, due to a lawful non-notification of the incident occurring to the DSP, the bigger the impact that will threaten the functioning of the essential service concerned.

The next section analyses the risk of legal fragmentation that can result from the potential overlap of cybersecurity and incident notification requirements between the NIS Directive and other existing breach-reporting duties under different pieces of EU legislation, such as the GDPR or the European

[391] Directive (EU) 2016/1148, Art. 17(1).

[392] Commission Implementing Regulation (EU) 2018/151 Article 3 specifies the parameters set out by Directive (EU) 2016/1148 Article 16(4) to be taken into account by the DSP to determine whether the impact of an incident is substantial (e.g., the DSP will be able to estimate the number of affected natural or legal persons with whom a contract for the provision of the service has been concluded or the number of affected users having used the service based on previous traffic data). Whereas Article 4 introduces quantitative thresholds in order to determine whether the impact is substantial: (a) at least 5M user-hours have to be affected by the incident in terms of availability of the service; (b) if the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data has to affect more than 100.000 users; (c) the incident has created a risk to public safety, public security or of loss of life; and, (d) the incident caused material damage to at least one user in the Union exceeding 1M euros.

[393] Cfr. for example, with ISO/IEC 27000:2016.

Electronic Communications Code (EECC). This issue is of particular concern to the stakeholders working within the extremely cross-sectoral IoT market[394].

Finally, section 3.2.2.2 addresses the limited scope of the Directive with regard to the exemption of hardware manufacturers and software developers: taking into special account the IoT domain[395], the question is whether it is desirable to address operators of essential services or digital service providers when either software or hardware vulnerabilities of IoT systems – which would eventually be part of the "network and information systems" of the NIS actor under scrutiny – are exploited by attackers, and, as a result, a security incident occurs. In other words, why and to what extent OESs (or DSPs) should be considered the best placed actors to draw up and implement the appropriate and proportionate *technical* and *organisational* measures to manage the risks posed to the security of IoT systems they use in their operations?

3.2.2 Aligning cybersecurity and incident notification requirements under different EU legislation

The NIS Directive's security and incident notification requirements – also known as cybersecurity breach reporting, breach reporting or breach notification – may overlap with other cybersecurity requirements and reporting duties under different EU legal instruments. Indeed, cybersecurity rules related to "network and information systems" already regulate – or will regulate in the future – certain sectors of the Market through sector-specific legal acts[396]. In order to avoid legal uncertainty, resulting from the fragmentation of the network and information systems security requirements, which would negatively impact the Single Market participants with overcomplicated compliance and increased in costs, Article 1(7) of the NIS Directive sets forth a general rule of prevalence of sector-specific EU legal acts over the provision of the Directive if they require OESs or DSPs "either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are *at least equivalent in effect* to the obligations laid down in this Directive, *those* provisions of that sector-specific Union legal act shall apply [emphasis added]"[397].

Ducuing remarkably breaks down this provision, highlighting internal inconsistencies. The obscure phrasing of the article would suggest that, when assessing the applicable regime, cybersecurity measures and cybersecurity incident reporting duties should be evaluated separately. It follows that

---

[394] Rolf H Weber and Evelyne Studer, 'Cybersecurity in the Internet of Things: Legal Aspects' (2016) 32 Computer Law and Security Review 715, 726.

[395] ibid.

[396] Directive (EU) 2016/1148, Recital 9.

[397] Directive (EU) 2016/1148, Article 1(7).

some sector-specific cybersecurity provisions could not meet the *equivalence* threshold set by the NIS Directive, while some others do (whether in terms of security measures or breach reporting), creating therefore concurrent application. "Concretely, where security requirements of EU sector-specific legislation would apply in lieu of NIS security provisions, remaining NIS notifications obligations would still be applicable, should there not be "at least equivalent" notification obligations in the EU sector-specific legislation"[398]. However, Ducuing argues that Recital 9 explicitly takes another view since it rules out[399] NIS Directive's identification process for those OESs to whom "at least equivalent"[400] cybersecurity requirements are already imposed by sector-specific legislation, precluding therefore the application of the NIS Directive altogether[401].

With specific regard to security incident reporting requirements, the NIS Cooperation Group[402] recently published a report aiming at investigating existing overlaps and possible synergies between a plethora of EU security incident reporting schemes[403]. Aligning and harmonising cybersecurity incident reporting simplifies reporting burdens for companies (e.g., compliance costs) and, on the other hand, helps national authorities in (i) saving costs; (ii) improving efficiency; (iii) achieving a better understanding of root causes and cross-sectoral impact; (iv) identifying and correlating cross-sectoral issues and effects; (v) enhancing cross-sectoral collaboration; (vi) exchanging good practices[404].

Accordingly, seven EU legal acts have been identified. Besides the NIS Directive, the pieces of EU legislation analysed by the report are Directive (EU) 2018/1972 (hereinafter, the EECC), Directive 2002/58/EC (ePrivacy Directive), Regulation (EU) 2016/679 (GDPR), Regulation (EU) 910/2014 (eIDAS Regulation), Directive (EU) 2015/2366 (PSD2 Directive) and Regulation (EU) 2017/745 (MDR). Without dwelling on a comparative analysis of the provisions of these legal acts too

---

[398] Charlotte Ducuing, 'Understanding the Rule of Prevalence in the NIS Directive: C-ITS as a Case Study' (2021) 40 Computer Law and Security Review 105514, 8 <https://doi.org/10.1016/j.clsr.2020.105514>.

[399] Directive (EU) 2016/1148, Recital 9: "Whenever those Union legal acts contain provisions imposing requirements concerning the security […] or notifications of incidents […], Member States should then apply the provisions of such sector-specific Union legal acts, including those relating to jurisdiction, and should not carry out the identification process for operators of essential services as defined by the Directive".

[400] Ducuing (n 45) 11: as regards the criterion that ought to be applied when assessing the equivalence of the cybersecurity requirements of the legal frameworks under scrutiny, in order to determine whether it should prevail over the NIS Directive, the author contends that the 'level of details' of the sector-specific legislation should consider whether "a legal framework takes into account the specificities of the sector, actors, technologies and more generally ecosystem at stake".

[401] ibid 8.

[402] Established by Directive (EU) 2016/1148 (art. 11) to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence.

[403] NIS Cooperation Group, 'Synergies in Cybersecurity Incident Reporting - CG Publication 04/20' (2020) <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>.

[404] ibid 20.

extensively, this section aims to cast light on the more specific interface, in terms of security breach reporting duties, between the NIS Directive, on the one hand, and, on the other, the EECC and the GDPR. Thus, the scope of these two legal acts is rather horizontal regarding the IoT market, as potentially applicable to every IoT deployment scenario. Conversely, the eIDAS Regulation[405], PSD2 Directive[406] and Regulation on Medical Devices[407] are too IoT sector-specific and therefore exceed the scope of the present work, as already underlined in the Methodology section.

Directive (EU) 2018/1972[408] is part of the revision of EU telecommunications legal framework within the Digital Single Market Strategy of the Commission. The rationale behind a European electronic communications code (EECC) is to harmonise, to the extent possible, all electronic communications networks and services, with the exception of content-related matters. Thus, the EECC "does not cover the content of services delivered over electronic communications networks using electronic communications services, such as broadcasting content, financial services and certain information society services"[409].

In this respect, the scope of the EECC shall be considered horizontal, or rather cross-sectorial, vis-à-vis the Internet of Things[410], regardless therefore of the different IoT sectors or verticals, as the Directive applies to electronic communication networks and services. The former are defined by article 2(1) as "transmission systems […] and, where applicable, switching or routing equipment and other resources […] which permit the *conveyance of signals* by wire, *radio*, optical *or other electromagnetic means*, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the

---

[405] Directive (EU) 2016/1148 Article 1(3) states that NIS Directive's security and notification requirements shall not apply to trusted service providers subject to the requirements of Article 19 of the eIDAS Regulation. Therefore, the prevalence of sector-specific legislation, ie Regulation 910/2014, over the NIS Directive is here operationalised by the Directive itself.

[406] European Commission, 'ANNEX to the COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Making the Most of NIS – towards the Effective Implementation of Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Info' (2017) 37 <https://eur-lex.europa.eu/resource.html?uri=cellar:d829f91d-9859-11e7-b92d-01aa75ed71a1.0001.02/DOC_4&format=PDF>, the European Commission concludes that "pursuant to Article 1(7) NIS Directive, both security and notification requirements set out in Article 95 and 96 of the PSD 2 should apply instead of the corresponding provisions of Article 14 of the NIS Directive".

[407] Elisabetta Biasin, 'The NIS2 Proposal: Which Regulatory Challenges for Healthcare Cybersecurity?' (*KU Leuven CiTiP blog*, 2021) <https://www.law.kuleuven.be/citip/blog/the-nis2-proposal-which-regulatory-challenges-for-healthcare-cybersecurity/>: "Medical Device Regulation (MDR) requirements on serious incidents may overlap with NIS2 provisions".

[408] DIRECTIVE (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

[409] Directive (EU) 2018/1972, Recital 7.

[410] Suada Hadzovic, 'Internet of Things from a Regulatory Point of View', *20th International Symposium INFOTEH-JAHORINA (INFOTEH)* (Institute of Electrical and Electronics Engineers Inc 2021).

purpose of transmitting signals" [emphasis added] [411]; and the latter being defined by article 2(4)(c) as " [also] services consisting wholly or mainly in the *conveyance of signals* such as transmission services used for the provision of machine-to-machine services and for broadcasting" [emphasis added][412].

The conveyance of (radio) signals is pivotal for underpinning the evolving wireless IoT communications technologies and applications in radio spectrum management[413]. Indeed, the overall aim of the regulatory framework is to cover the use of radio spectrum "by all electronic communications networks, including the emerging self-use of radio spectrum by new types of networks consisting exclusively of autonomous systems of mobile radio equipment that is connected via wireless links without a central management or centralised network operator recitals"[414]. Unsurprisingly, the EECC framework pose several regulatory challenges for the telecom sector that could eventually hinder the deployment of IoT in EU, in terms of legal uncertainty about scope and definitions (for example, the definition of "conveyance of signals" may prove to be troublesome when it comes to IoT transmissions services that are bundled with other types of services; or the exclusion from the rules related to interpersonal communication services, whereby an IoT service includes interpersonal communication only as an "ancillary feature" to the main service)[415] and lack of harmonisation[416].

Coming now to the cybersecurity and incident notification requirements under the EECC, Article 40 lays down the legal basis for the security of network and information systems of electronic communication networks and services providers. Similar to the OESs' cybersecurity requirements under the NIS Directive, the providers of public electronic communications networks or of publicly available electronic communications services, having regard to the state of the art, shall take appropriate and proportionate technical and organisational measures, such as encryption, to appropriately manage the risks posed to the security of networks and services[417]. Notwithstanding the cybersecurity risk management, if a security incident *significantly* impacts on the operation of

---

[411] Directive (EU) 2018/1972, Article 2(1).

[412] Directive (EU) 2018/1972, Article 2(4)(c).

[413] Directive (EU) 2018/1972, Recital 30.

[414] Directive (EU) 2018/1972, Recital 12.

[415] Vodafone, 'A New IoT Regulatory Framework for Europe' (2019) <https://investors.vodafone.com/sites/vodafone-ir/files/vodafone/our-purpose/social-contract/policy-papers/a-new-iot-regulatory-framework-for-europe.pdf>; Hogan Lovells, 'A Comparison of IoT Regulatory Uncertainty in the EU China and the United States' (2019) <https://www.hlmediacomms.com/files/2019/03/Hogan-Lovells-A-comparison-of-IoT-regulatory-uncertainty-in-the-EU-China-and-the-United-States-March-2019.pdf>.

[416] To make things worse, on 4 February 2021, the EU Commission opened infringement procedures against 24 Member States for not transposing the EECC: <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_206>.

[417] Directive (EU) 2018/1972, Article 40(1).

networks or services, the providers have to notify to the competent authorities without undue delay[418]. Interestingly, the notification duties under the EECC goes beyond the provision of article 14 of the NIS Directive to include threats[419]. The alignment and harmonisation assessment between the NIS Directive and the EECC, as regards security and incident notification requirements of specific NIS Directive's OESs like EECC's providers of public electronic communications networks or of publicly available electronic communications services, is carried out by the former at article 1(3), whereby a rule of prevalence of articles 13a and 13b of Directive 2002/21/EC – then repealed by the EECC – over the security and notification requirements of the NIS Directive is established[420].

Conversely, as far as the NIS Directive and the GDPR are concerned, the potential overlap between these two legal instruments is threefold at least, regarding (i) the risk-based security measures; (ii) the incident notification obligations; and (iii) the processing of personal data under the NIS Directive[421]. This section investigates to what extent the coexistence of the incident notification obligations arising from the two different regimes, which have different scope (i.e., the security of network and information systems and the protection of natural persons' fundamental rights and freedoms, in particular, with regard to their right to the protection of personal data), may prove to be troublesome for all the stakeholders involved: the national competent authorities, the reporting entities, and finally the individuals concerned.

Under the GDPR, a data controller has the duty to notify a personal data breach, without undue delay[422] and no later than 72 hours after becoming aware of it[423], to the supervisory authority unless the incident is unlikely to result in a *risk* to the rights and freedoms of individuals[424] and to the data

---

[418] Directive (EU) 2018/1972, Article 40(2). To determine the significance of the incident, the EECC lays down five parameters: (a) the number of users affected by the security incident; (b) the duration of the security incident; (c) the geographical spread of the area affected by the security incident; (d) the extent to which the functioning of the network or service is affected; (e) the extent of impact on economic and societal activities.

[419] Directive (EU) 2018/1972, Article 40(3); Serge JH Gijrath, '(Re-)Defining Software Defined Networks under the European Electronic Communications Code' (2021) 40 Computer Law & Security Review 10.

[420] Directive (EU) 2016/1148, Article 1(3); Sandra Schmitz-Berndt and Fabian Anheier, 'Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context' (2021) 7 European Data Protection Law Review 101, 104 <https://edpl.lexxion.eu/data/article/16999/pdf/edpl_2021_01-014.pdf> accessed 26 October 2021.

[421] Cole and Schmitz (n 381).

[422] Regulation (EU) 2016/679, Article 33(1): if the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

[423] Regulation (EU) 2016/679, Recital 87: "[t]he fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject".

[424] Regulation (EU) 2016/679, Article 33(1). Article 33(3) lays down the minimum information that must inform the notification: (a) the nature of the personal data breach, the categories and number of data subjects and personal data records concerned; (b) the contact details of the data protection officer; (c) the likely consequences that follow the breach; (d) the measures taken or proposed by the controller to address the personal data breach.

subjects concerned if the breach is likely to result in a *high risk* to their rights and freedoms[425]. Not surprisingly, the GDPR defines a personal data breach as 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"[426]. Indeed, as stressed in Chapter two, the fundamental rights of privacy and data protection depend on *some* cybersecurity technologies, as not every security technology should be framed as fundamental rights *infraethical* facilitator.

Provided this logical and technical nexus between cybersecurity measures and personal data protection, it is non-contended that a cybersecurity incident would most of the times involve a personal data breach. Certainly, these incidents shall be distinguished in terms of the affected assets – as cybersecurity incidents may not involve personal data breaches[427] – and the protection regime they would trigger. The same incident in fact would fall under the scope of both the NIS Directive and the GDPR if it *significantly* or *substantially* affects an OES or a DSP and, at the same time, leads "to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Whether this is the case, "the same incident may be reported to two separate regulators under different reporting schemes and notably with different objectives"[428], even by two different entities, giving rise potentially to conflicts and confusion. As a consequence, different authorities will receive diverging information with regard to a single incident and […] one incident may be treated as if there were separate"[429].

To make things more complex, on a lower level of abstraction, the diverging incident notifications timeline under the NIS and the GDPR may add further problems, as early notifications to the data subjects might jeopardise the cybersecurity operations aiming at minimising or recovering from the breach[430]. On the one hand, recital 86 GDPR acknowledges the need to counter a cyberattack as a justification to delay the communication to the data subject pursuant to Article 34 GDPR; on the other, "the justification is limited to continuing and ongoing data breaches and does not encompass

---

[425] Regulation (EU) 2016/679, Article 34(1). Article 34(3) contains an exception to the first paragraph. The notification is not required if (a) the controller has implemented appropriate technical and organisational measures that render the personal data intelligible to unauthorised parties; (b) the controller has taken subsequent measures ensuring that the *high risk* is no longer likely to materialise; (c) the effort to notify would be disproportionate: in such case, there shall be a public communication or similar measure.

[426] Regulation (EU) 2016/679, Article 4(12).

[427] Cédric Burton, 'Article 33 Notification of a Personal Data Breach to the Supervisory Authority' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 645.

[428] Schmitz-Berndt and Anheier (n 420) 101.

[429] ibid 105.

[430] Sandra Schmitz-Berndt and Stefan Schiffner, 'Don't Tell Them Now (or at All)–Responsible Disclosure of Security Incidents under NIS Directive and GDPR' (2021) 35 International Review of Law, Computers and Technology 101 <https://doi.org/10.1080/13600869.2021.1885103>.

ongoing security incidents as such, [falling] short in an incident which incidentally compromised consumer data but leads to an ongoing attack targeted at other vital systems of the OES or DSP"[431]. Therefore, "the mitigation of the impact of a cybersecurity incident in the context of compromised personal data, may thus require the cooperation of the competent NCA (national competent authority) and DPA (data protection authority)"[432].

As already addressed by Chapter two in the context of the public good doctrine for cybersecurity, it is becoming increasingly clear that *cooperation*, *coordination*, *experience* and *information-sharing* are needed elements when facing cyberattacks. A lack of collaboration and information sharing between the authorities under the NIS Directive and GDPR regimes might seriously hamper the rationale underlying the notification requirements of the two legal acts. In this respect, some have argued that it would be appropriate to have a single point of contact for notifications, which may then inform the appropriate authority or authorities of a security incident involving personal data[433]. Against this background, the Proposal for a revised NIS Directive[434] – which will form the analysis of section 3.1.2 – explicitly addressed this issue. Recital 56 of the so-called NIS 2.0 reads as follows:

> *Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies*[435].

[431] ibid 9–10.

[432] Schmitz-Berndt and Anheier (n 420) 105.

[433] Cole and Schmitz (n 381) 20.

[434] European Commission, Proposal for a Directive of the European Parliament and of the Council on measure for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020) 823 final).

[435] ibid, Recital 56.

3.2.3 The NIS Directive's exclusion of hardware manufacturers and software developers

This section addresses yet another key challenge of the EU governance of cybersecurity, that is, "to impose the right obligations on the right actors, through the right instrument"[436]. In particular, the exclusion of hardware manufacturers and software developers from the scope of the NIS Directive might enlighten a regulatory failure that negatively impacts the IoT market. Recital 50 of the NIS Directive, albeit not legally binding[437], explicitly exclude from the scope of the Directive hardware manufacturers and software developers, as (i) they are not OESs nor DSPs; and (ii) the European legislator considered the existing rules on product liability to be sufficient[438].

The impact of the so-called emerging digital technologies (such as AI or the IoT) on the EU product liability rules, notably Directive (EU) 85/374/EEC ("Product Liability Directive)[439], has received wide attention by both legal scholars[440] and EU institutions[441]. The question whether the Product Liability Directive could play a role within the allocation of liability, stemming from cybersecurity vulnerabilities, of the variety of actors involved in the IoT chain – such as hardware manufacturer or

---

[436] Fuster and Jasmontaite (n 180) 109.

[437] Tadas Klimas, 'The Law of Recitals in European Community Legislation' (2008) 15 ILSA Journal of International & Comparative Law 61.

[438] Directive (EU) 2016/1148, Recital 50.

[439] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[440] See *inter alia* Duncan Fairgrieve and others, 'Product Liability Directive' in Piotr Machnikowski (ed), *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (Intersentia 2017); Cees van Dam, *European Tort Law* (Second ed., Oxford University Press 2013); Magdalena Tulibacka, *Product Liability Law in Transition: A Central European Perspective* (Routledge 2016); ROBOLAW, 'Final Report Summary - Regulating Emerging Robotic Technologies in Europe: Robotics Facing Law and Ethics' (2014) <https://cordis.europa.eu/project/id/289092/reporting> accessed 22 November 2021; Jean-Sebastien Borghetti, 'How Can Artificial Intelligence Be Defective?' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things - Münster Colloquia on EU Law and the Digital Economy IV* (Bloomsbury Publishing 2019); Miquel Martìn-Casals, 'Causation and Scope of Liability in the Internet of Things (IoT)' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things - Münster Colloquia on EU Law and the Digital Economy IV* (Bloomsbury Publishing 2019); Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* (Springer 2013); Giovanni Sartor and Andrea Omicini, 'The Autonomy of Technological Systems and Responsibilities for Their Use' in Nehal Bhuta and others (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press 2016); Rolf H Weber, 'Liability in the Internet of Things' (2017) 6 Journal of European Consumer and Market Law 207.

[441] The European Parliament issued a Resolution calling for updated civil liability rules: European Parliament, 'Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics' (2017). The European Commission then published a document to provide a first mapping of liability challenges that occur in the context of emerging digital technologies: European Commission, 'Commission Staff Working Document - Liability for Emerging Digital Technologies - Accompanying the Document: Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee' (2018). Moreover, in March 2018 the EC appointed a group of experts to provide the Commission with expertise on the applicability of the Product Liability Directive to traditional products, new technologies and new societal challenges. The report of November 2019, is the final deliverable of the Expert Group on "Liability and New Technologies": European Commission Expert Group on Liability and New Technologies, 'Liability for Artificial Intelligence and Other Emerging Digital Technologies' (2019).

software developer – would exceed the scope of the thesis since it would require an analysis of traditional theories of tort law[442].

Rather, the question worth asking is whether it is fair to hold OES and DSP responsible – and ultimately liable – for cybersecurity incidents that are likely to be beyond their control. This could be the case if intrinsic IoT vulnerabilities that could not be mitigated by the OES in question – either at device (hardware) or network and application (software) level – are successfully exploited by an attacker. By holding NIS actors responsible for such incidents, rather than directly addressing the actors in charge of security features' design and implementation which will eventually affect OESs' and DSPs' network and information systems, the problem of *insecure* IoT devices is "not addressed at the core"[443]. In this respect, the remaining sections of this Chapter address the revision process of EU product safety legislation and recent initiatives undertook by the Commission (in particular, the revision of the NIS Directive and the Cyber Resilience Act) with a view of tackling the issue of connected devices cybersecurity.

To make things worse, this exclusion could hinder the efforts to enhance overall IoT cybersecurity with regards to supply chain. The majority of IoT devices is thus comprised of many components from different hardware and software vendors, part of which could even be accounted for by small companies, including start-ups – excluded from the scope of the NIS Directive too[444]. Chapter 1 already showed how IoT expands the global attack surface disproportionately due to the variety of integrated and interconnected products and manufacturers. Recent discussions, both in Europe and in the US, find a consensus that IoT supply chain security is crucial: ENISA and the US National Institute of Standards and Technology (NIST) acknowledge that the supply chain represents a challenge and an opportunity. On the one hand, it lays down the foundation for devices' security and, on the other hand it raises concerns since organisations are hardly aware of the security measures adopted by supply chain partners[445]. ENISA maps out the entire lifespan of IoT supply chain –

---

[442] Lieke Anne Josephine Sterk, 'The Hacker, Product Manufacturer, Sensor Manufacturer, Software Provider or Infrastructure Provider?' [2018] Thesis LLM Law and Technology Tilburg Law School <http://arno.uvt.nl/show.cgi?fid=145943>; Pier Giorgio Chiara, 'Sistemi Intelligenti Autonomi e Responsabilità Civile: Stato Dell'arte e Prospettive Nell'esperienza Comunitaria' (2020) 1 Diritto ed Economia dell'Impresa 105.

[443] Sterk (n 442) 32.

[444] Directive (EU) 2016/1148, Article 16(11) states that Chapter V i.e., security of the network and information systems of digital service providers, does not apply to micro and small enterprises; see https://www.startus-insights.com/innovators-guide/5-top-internet-of-things-startups-impacting-logistics-supply-chain/; European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions An SME Strategy for a Sustainable and Digital Europe COM(2020) 103 Final' (2020) 1.

[445] ENISA, 'Guidelines for Securing the Internet of Things - Secure Supply Chain for IoT' (n 142) 5; Megas, Fagan and Lemire (n 143) 13.

hardware, software and services – by offering security measures for each step[446]. The need to "secure" the entire IoT supply chain is making it much harder for the stakeholders involved in IoT cybersecurity – notably, OESs pursuant to article 14 of the NIS Directive – to fulfil their duties in managing vulnerabilities and risks.

Ironically, the Directive acknowledges the important role played by hardware manufacturers and software developers[447]. Their products (and services) are the backbone of the network and information systems infrastructure of OESs and DSPs[448]. They are thus crucial in enabling OESs and DSPs to enhance the security of their NIS infrastructure. In fact, hardware manufacturers and software developers of IoT solutions actually maintain a pivotal role during the lifecycle of their devices. IoT devices frequently contact several actors for manifold reasons (e.g., updates, data processing, functionality reports, etc.): there is a large consensus in the literature in considering the manufacturer of the device as a first party, whilst cloud service providers are usually classified as support parties, among the manifold machine communication's destinations[449].

The central role of manufacturers and developers vis-à-vis the state of systems' cybersecurity has been highlighted by ENISA's gap analyses several times. NIS Directive's goal of managing cybersecurity risks through appropriate and proportionate security measures can only be effectively if pursued *via* the involvement of vendors, "since they are in charge of designing and developing the devices, they are in an ideal position to implement the changes needed – they are able to proficiently and cost-efficiently include new security features or characteristics. […] Through their lifecycle, IoT devices must be able to be patched and updated rapidly to ensure their correct operation and to amend all the vulnerabilities that are continuously being discovered"[450].

Accordingly, the objective of managing the number and severity of IoT vulnerabilities – and risks – should change by shifting the emphasis from deployment of security measures and controls in a later phase by "indirect" actors (i.e., OESs), towards an effective and proactive systems' designing and developing, having therefore 'security in mind'. Several security challenges of the IoT can be addressed by manufactures and developers by establishing a set of secure development guidelines i.e., Software Development Life Cycle principles, such as checking for security vulnerabilities, secure

---

[446] ENISA, 'Guidelines for Securing the Internet of Things - Secure Supply Chain for IoT' (n 142) 9.

[447] Directive 2016/1148, recital 50.

[448] Weber and Studer (n 394).

[449] Anna Maria Mandalari and others, 'Towards Automatic Identification and Blocking of Non-Critical IoT Traffic Destinations' (2020) <http://arxiv.org/abs/2003.07133>.

[450] ENISA, 'Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures' (n 1) 56.

deployment, ensuring continuity of secure development in cases of integrators, continuous delivery etc.[451]

Nevertheless, IoT manufacturers and vendors "usually consider functionality and usability much more important than implementing secure design and programming [:] the main reason for these companies no to dedicate much of their budget to security is the general perception that there is no direct return-on-investment for security, which can be attributed to the economic cost and the difficulty to assess"[452]. From a legal-economic perspective, the lack of incentives that eventually hinders the development of secure IoT solutions are not only purely economic[453] but legal as well. Thus, a growing number of OES and DSP believe that implementing the NIS Directive has strengthened their detection capabilities and their ability to recover from incidents, while the compliance process required additional budget[454].

The current legal *formula* of the NIS Directive would burden the cost of an incident on a party (i.e., the OES) who is unable to reduce the probability of the occurring (security) incident[455] in the same way as the producer. Notwithstanding the lack of legal obligations under the NIS Directive, the latter are undoubtedly better placed to adopt cybersecurity measures to manage the risks posed to their products and services than OESs. In accordance with the theoretical framework addressing "cybersecurity as public good" in Chapter 2, increased sharing NIS responsibilities[456] to be borne by IoT vendors would create legal incentives to implement secure design and development.

In the review process of the NIS Directive, different stakeholders have been commented on the Commission's inception impact assessment and roadmap for the adoption of a new NIS Directive[457]. Against the background of an expanded scope, having particular regard to the inclusion of software vendors, BSA argued that such market sector was already cover "within the Cloud services' inclusion in Annex III, notably through the Software As A Service principle. For the very limited cases where a software would not be delivered or serviced through the cloud (i.e. when embedded), the incident reporting obligations would be irrelevant, as the manufacturer would not have the visibility of the

---

[451] ENISA, 'Good Practices for Security of IoT Secure Software Development Lifecycle' (2019) 7 <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1>.

[452] ENISA, 'Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures' (n 1) 55.

[453] ibid.

[454] ENISA, 'NIS Investments' (2021) 66–67 <https://www.enisa.europa.eu/publications/nis-investments-2021> accessed 27 November 2021.

[455] Guido Calabresi, *The Cost of Accidents - A Legal and Economic Analysis* (Yale University Press 1970).

[456] The reference here is to the duties enshrined in Article 14 of the NIS Directive.

[457] See <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems_it> accessed 4 December 2021.

incident affecting that specific piece of software"[458]. It is highly debatable whether the cases of 'embedded software', that is, not cloud-based, are 'limited' in the increasingly evolving market of IoT, robotics and AI. Moreover, even assuming that this is the case, BSA only accounts for security breaches reporting duties (regarding them as irrelevant), completely ignoring security measures requirements. On the contrary, GSMA firmly supports the need to include in the scope of the revised NIS Directive software developers and hardware manufacturers to ensure robust end-to-end security. "Such extension of the NIS Directive would ensure that each actor takes responsibility for their part in a secure and resilient digital value chain. Overall, introducing clear legal requirements (notably security and notification requirements) on these actors will help to achieve a higher level of cybersecurity in the EU"[459].

In conclusion, this section demonstrated that the lack of legal obligations on hardware and software manufacturers and developers in terms of 'products' cybersecurity has a negative impact on OESs. However, addressing this regulatory gap with the legal instrument of the NIS Directive is not the right answer. Thus, the principle-based model of governance of the NIS was not meant to cover product-related requirements, which are already contained in product safety legislation as will be addressed in section 3.4. Rather, it focuses on administrative and organisational aspects (e.g., laying down a procedural framework for the notification of incidents having a significant or substantial impact on the network and information systems of the entities in scope). Against this backdrop, section 3.6 casts light on the recent EC initiative for a Cyber Resilience Act which would directly tackle the problem of unsecure connected devices by setting forth common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products and ancillary services.

3.3 Cybersecurity Certification Schemes

3.3.1 The Cybersecurity Act: exploring EU voluntary cybersecurity certification legal framework

The European Commission published in 2017 – just after the entry into force of the NIS Directive – its second Cybersecurity Strategy[460]. In order to scale up EU's cybersecurity preparedness and

[458] BSA The Software Alliance, 'Comments on EU Commission's NIS Directive Review' (*2020*) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F543319_it> accessed 3 December 2021.

[459] GSMA, 'Consultation on the Revision of the NIS Directive' (2020) 12 <https://www.gsma.com/gsmaeurope/wp-content/uploads/2020/10/GSMA-Response-to-EC-public-consultation-on-NIS-Review.pdf> accessed 3 December 2021.

[460] European Commission, 'Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU' (2017) <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017JC0450> accessed 30 November 2021.

improve IoT connected devices' robustness and resilience, whose security is not yet prioritised in the design phase, the Commission proposed a permanent status, alongside a stronger mandate, for the ENISA and the "establishment of an EU cybersecurity certification framework that will ensure the trustworthiness of the billions of devices ("Internet of Things") which drive today's critical infrastructures, such as energy and transport networks, and also new consumer devices, such as connected cars"[461].

Especially in a technical field such as cybersecurity[462], certifications build up on security technical standards[463], which are "the most effective tool to introduce technical requirements without overly prescriptive normative provisions that might become outdated as technology evolves"[464]. In other words, given that hardware and software manufacturers and developers – and, therefore, 'IoT manufacturers' – are excluded from the scope of the NIS Directive, certifications, albeit voluntary, would be an instrument to achieve legislative goals[465], that is, enhancing the cybersecurity posture of these stakeholders by encouraging them to implement measures at the earliest stages of design and development of their products, services and processes. The sectors regulated by Directive (EU) 2016/1148 are domains in which cybersecurity certification is critical[466]. ENISA report on 'NIS investments' highlights a strong correlation – which does not necessarily imply causation – between "a very positive self-perception of cybersecurity maturity and the existence of cybersecurity certifications for processes, people and products. Organisations that certify their staff and systems and buy products with cybersecurity certifications are 36.36 % more likely to self- assess their cybersecurity maturity as 'far above industry standards'"[467].

---

[461] European Commission, 'State of the Union 2017 - Cybersecurity: EU Agency and Certification Framework' (2017) 1 <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193>.

[462] The interface between IoT and standards is not limited to the field of cybersecurity. Within Intellectual Property and Competition Law, see *inter alia* Oscar Borgogno and Giuseppe Colangelo, 'SEPs Licensing Across the Supply Chain: An Antitrust Perspective' [2021] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3766118> accessed 29 November 2021.

[463] Constant Kohler, 'The EU Cybersecurity Act and European Standards: An Introduction to the Role of European Standardization' (2020) 1 International Cybersecurity Law Review 7 <https://link.springer.com/article/10.1365/s43439-020-00008-1> accessed 4 November 2021; ENISA, 'Standardisation in Support of the Cybersecurity Certification: Recommendations for European Standardisation in Relation to the Cybersecurity Act' (2019); AIOTI, 'AIOTI Position on the EU Cybersecurity Act Proposal' (2018) <https://euagenda.eu/publications/aioti-position-on-the-eu-cybersecurity-act-proposal> accessed 8 December 2021.

[464] Digital Europe, "Defining the way forward for IoT security and certification schemes" (2019) white paper, 5, available at: https://www.digitaleurope.org/resources/defining-the-way-forward-for-iot-security-and-certification-schemes/

[465] Irene Kamara, 'Misaligned Union Laws? A Comparative Analysis of Certification in the Cybersecurity Act and the General Data Protection Regulation' in Dara Hallinan, Ronald Leenes and Paul De Hert (eds), *Data protection and Privacy: Data Protection and Artificial intelligence* (Hart Publishing 2021) 85.

[466] Regulation (EU) 2019/881, recital 65.

[467] ENISA, 'NIS Investments' (n 454) 67.

In this respect, this section focuses on the question whether and to what extent the European cybersecurity certification framework, established by Regulation 2019/881[468], addresses legal uncertainty and closes regulatory gaps vis-à-vis IoT security addressed in the previous sections.

Against this backdrop, *cybersecurity law* shall be considered as a privileged interface in which we can better appreciate the paradigm shift in the EU's institutional landscape, from a European Law perspective, elsewhere described as 'agencification'. "EU agencies – like ENISA - are also increasingly authors of standards to be used in implementation of EU law by Member States. These roles of agencies have developed next to and alongside the more 'traditional' approach of regulatory law, which consists of references to 'outside' standards set by private and semi-private standardisation bodies and scientific expertise"[469]. As remarkably put by Busch, "standards are means by which we construct realities [, means] of *partially* ordering people and things so as to produce outcomes desired by someone. As such, they are part of the technical, political, social, economic, and ethical infrastructure that constitutes human societies"[470]. Whereas a broader understanding of the concept of 'standard' underpins this thesis, that is, standards as means that normatively mediate interactions between individuals[471], this section explores the strand underlined by the definition of 'standard' outlined in Article 2(1) of Regulation (EU) 1025/2012[472] i.e., a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory.

As noted by Gonzalez Fuster and Jasmontaite, EU's 'cybersecurity area' "revives itself by both law and inter-area policy measures. Policy measures from various policy areas eventually led to changes and adjustments in various EU legal frameworks and *vice versa*"[473]. Section 3.1 already demonstrated the pivotal role played by the first Cybersecurity Strategy (2013) of the Commission in EU cybersecurity legislation: the policy objectives were achieved notably in the adoption of the NIS

---

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

[469] Herwig CH Hofmann, 'European Regulatory Union? The Role of Agencies and Standards'' in Panos Koutrakos and Jukka Snell (eds), *Research Handbook on the EU's Internal Market* (Elgar Publishing 2016) 13.

[470] Lawrence Busch, *Standards: Recipe for Reality* (2011) MIT Press, 13; see also Janet Abbate, *Inventing the Internet* (MIT Press 1999).

[471] Massimo Durante, "Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks" (2019) in Don Berkich, Matteo D'Alfonso (Eds.) *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence*, 134 Philosophical Studies Series, Springer.

[472] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.

[473] Fuster and Jasmontaite (n 180) 101.

Directive. And the Second Cybersecurity Strategy makes no difference. Eventually, the course of action proposed by the Commission in 2017 resulted in Regulation (EU) 2019/881, also known as the Cybersecurity Act. Interestingly, this is the first legal act that provides for a definition of 'cybersecurity', which differs substantially from the one enshrined in the Cybersecurity Strategy of 2013: "cybersecurity means the activities necessary to protect network and information systems, *the users of such systems and other persons affected by cyber threats* [emphasis added]"[474]. Whereas the previous conceptualisation insisted on the cyber domain and, therefore, on the threats that could harm the underlying network and information infrastructure, the new understanding of 'cybersecurity' broadens the perimeter, echoing the substance of the considerations contained in Chapter 2, to include not only the users of NIS but *any other persons,* and possibly their (fundamental) rights, that may be affected by cyber threats, going above and beyond information security's CIA triad dependency of the 2013 definition.

The Cybersecurity Act has mainly two focal areas. The first, from Article 3 to 45, reshapes ENISA's critical position in defending the digital ecosystem of the Union[475], whereas the second, from Articles 46 to 65, establishes the European cybersecurity certification legal framework. In face of the changed and rapidly evolving cybersecurity landscape, the Commission deemed it necessary to enhance ENISA's role, with new objectives[476] and tasks[477]. The Agency is given a permanent mandate[478] and will "act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders"[479].

The European cybersecurity certification framework should serve a twofold purpose: it should (i) increase trust in ICT products, services and processes that have been certified under European cybersecurity certification schemes (ECCS) and, (ii) avoid the multiplication of conflicting or overlapping national cybersecurity certification schemes and thus reduce costs for undertakings operating in the digital single market[480].

---

[474] Regulation (EU) 2019/881, Article 2(1).

[475] Regulation (EU) 2019/881, Recital 19.

[476] Article 4 of Regulation (EU) 2019/881 outlines the main objectives of the Agency, such as assisting Union institutions, bodies, offices, agencies as well as Member States in implementing EU policies on cybersecurity, supporting capacity-building and preparedness across the Union, promoting cooperation, including information-sharing and coordination at Union level, contributing to increasing cybersecurity capabilities and promoting the use of EU cybersecurity certification.

[477] Article 5 of Regulation (EU) 2019/881 mainly refers to 3 strands of actions: *assisting* in the development, review, implementation of Union cybersecurity policy and law; *contributing* to the work of the Cooperation group; *supporting* the development and implementation of cybersecurity policy in Union legislation as well as the regular review of Union policy through an annual report on the state of the implementation of the respective legal framework.

[478] Regulation (EU) 2019/881, Article 68(4).

[479] Regulation (EU) 2019/881, Article 3(1).

[480] Regulation (EU) 2019/881, Recital 69.

The Cybersecurity Act considers that the insufficient adoption of the principle of 'security by design' hinders IoT cybersecurity. In this respect, the limited use of certification schemes contributes to information asymmetries underlying consumers' insufficient understanding of the overall security of ICT products, processes and services[481]. Thus, the regulation relies on the assumption that full realisation of the Digital Single Market may be hindered by a lack of trust in the cybersecurity level of ICT products, services and processes[482], due to insufficient information about the security features of such solutions[483]. Without entering into an epistemological discussion on the meaning of 'trust'[484], in less problematic terms it can be assumed that here, 'trust', refers to the (successful) delegation to third parties, whether national cybersecurity certification authorities[485], conformity assessment bodies[486] or manufacturers themselves[487], of the conformity evaluation procedure that ICT products, services and processes must undergo in order to be certified.

In other words, the certification mechanism is seen as a means to enhance consumers trust through a proof of conformity "with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle"[488]. It follows that trust, in the certification context, is associated with transparency[489]; or, rather, the latter is a proxy for the former.

Conversely, the risk of fragmentation – despite some efforts made with a view to ensuring mutual recognition of certificates within the Union, such as the Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA)[490] – is particularly felt in the IoT domain, as testified by the wording of Recital 67 CSA:

> *"Currently, the cybersecurity certification of ICT products, ICT services and ICT processes is used only to a limited extent. When it exists, it mostly occurs at Member*

---

[481] Regulation (EU) 2019/881, Recital 2.

[482] Regulation (EU) 2019/881, Recital 65.

[483] Regulation (EU) 2019/881, Recital 2.

[484] Durante, *Computational Power: The Impact of ICT on Law, Society and Knowledge* (n 83) 29–30.

[485] Regulation (EU) 2019/881, Article 58.

[486] Regulation (EU) 2019/881, Article 60.

[487] Regulation (EU) 2019/881, Article 53.

[488] Regulation (EU) 2019/881, Article 46(2).

[489] Kamara (n 465) 98–99; Dayana Spagnuelo, Ana Ferreira and Gabriele Lenzini, 'Accomplishing Transparency within the General Data Protection Regulation', *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)* (2019) <https://www.datenschutzzentrum.de/uploads/sdm/> accessed 2 December 2021; Konrad Stahl and Roland Strausz, 'Certification and Market Transparency ' (2017) 84 Review of Economic Studies 1842.

[490] See <https://www.sogis.eu/> accessed 1 December 2021.

State level or in the framework of industry driven schemes. In that context, a certificate issued by a national cybersecurity certification authority is not in principle recognised in other Member States. Companies thus may have to certify their ICT products, ICT services and ICT processes in several Member States where they operate […], which thereby adds to their costs. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach to horizontal cybersecurity issues, for instance in the field of the IoT. Existing schemes present significant shortcomings and differences in terms of product coverage, levels of assurance, substantive criteria and actual use, impeding mutual recognition mechanisms within the Union"[491].

Article 8 CSA arguably constitutes a direct interface between the two parts of the Regulation as ENISA is tasked to support and promote the development and implementation of EU policy on cybersecurity certification by preparing[492] a candidate scheme or reviewing[493] an existing European cybersecurity certification scheme for ICT products, services and processes (including, as previously addressed in Chapter 1, IoT systems[494]) – following a request from the Commission[495] on the basis of the 'Union rolling work programme'[496] or from the European Cybersecurity Certification Group (ECCG)[497], even without referencing the rolling work programme[498], the latter being however non-binding for the Agency[499].

When preparing the scheme, in adherence to a formal, open, transparent and inclusive consultation process typical of the consensus-based standardisation process[500], ENISA will consult all relevant stakeholders[501], in particular, having regard to the opinion of the ECCG that assist and advise ENISA

[491] Regulation (EU) 2019/881, recital 67.

[492] Regulation (EU) 2019/881, article 8(1)(b).

[493] Regulation (EU) 2019/881, article 48.

[494] Stefan Hessel and Andreas Rebmann, 'Regulation of Internet-of-Things Cybersecurity in Europe and Germany as Exemplified by Devices for Children' (2020) 1 International Cybersecurity Law Review 27, 32 <https://link.springer.com/article/10.1365/s43439-020-00006-3> accessed 4 November 2021.

[495] Regulation (EU) 2019/881, article 48(1).

[496] Regulation (EU) 2019/881, article 47(1): EU Commission's yearly publication which identifies strategic priorities for future ECCS.

[497] Regulation (EU) 2019/881, article 62(2): the ECCG is composed of representatives of national cybersecurity certification authorities or other relevant national authorities.

[498] Regulation (EU) 2019/881, article 48(2).

[499] Regulation (EU) 2019/881, article 49(2).

[500] Knut Blind, 'The Impact of Standardisation and Standards on Innovation' in Jakob Edler and others (eds), *Handbook of Innovation Policy Impact* (Edward Elgar Publishing Ltd 2016).

[501] Regulation (EU) 2019/881, article 49(3).

without binding force[502]. ENISA then transmits the candidate scheme to the Commission which may adopt it through an implementing act[503]. Once the implementing act is adopted, it produces a so-called 'standstill obligation', in a similar way to EU technical harmonisation[504], since the national cybersecurity certification schemes with the same scope of the ECCS cease to produce effects[505].

From a substantive legal standpoint, the Cybersecurity Act lays down cybersecurity certifications' minimum objectives and content. Unsurprisingly, Article 51 does not limit itself to encompassing classical computer and information security principles i.e., the CIA triad[506] and authentication[507], but also broadens the goals of cybersecurity certification schemes to cover more comprehensively cornerstone aspects of cybersecurity such as: handling of vulnerabilities[508], basic digital forensics principles[509], disaster recovery[510], security by design and by default[511], and software & hardware updates[512]. The regulation provides for a detailed, non-exhaustive list of necessary elements that schemes must contain, such as the scope and object of the certification (including the categories of ICT products, services and processes covered) or how the selected standards or technical specifications – that is, the detailed specification of the cybersecurity requirements, evaluation methods and the intended assurance levels ('basic', 'substantial' or 'high') correspond to the needs of the intended users of said scheme[513].

Recourse to EU cybersecurity certification is, *in principle*, voluntary. Thus, certifications are in essence voluntary private law instruments, as demonstrated in Article 42(3) GDPR[514] in the context of EU data protection law. Nevertheless, the nature of cybersecurity certification deviates significantly. The European legislator stipulates that Union law, or Member State law – adopted in accordance with Union law – may derogate from the general rule[515]. Moreover, in the absence of harmonised Union law, "Member States are able to adopt national technical regulations providing for

---

[502] Regulation (EU) 2019/881, articles 49(5), 49(6), 62(4).

[503] Regulation (EU) 2019/881, Article 49(7).

[504] Kamara (n 465) 89.

[505] Regulation (EU) 2019/881, Article 57(1).

[506] Regulation (EU) 2019/881, Article 51, letters (a) and (b).

[507] Regulation (EU) 2019/881, Article 51, letter (c).

[508] Regulation (EU) 2019/881, Article 51, letters (d) and (g).

[509] Regulation (EU) 2019/881, Article 51, letters (e) and (f).

[510] Regulation (EU) 2019/881, Article 51, letter (h).

[511] Regulation (EU) 2019/881, Article 51, letter (i).

[512] Regulation (EU) 2019/881, Article 51, letter (j).

[513] Regulation (EU) 2019/881, Article 54(1); Recital 84.

[514] Regulation (EU) 2016/679, Article 42(3): "the certification shall be voluntary and available via a process that is transparent".

[515] Regulation (EU) 2019/881, Article 56(2); Recital 91.

mandatory certification under a European cybersecurity certification scheme in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council"[516]. Thus, the Commission did not want to rule out the possibility of imposing specific cybersecurity requirements *via* mandatory certification with the aim of enhancing the Union's level of cybersecurity, taking into particular account the existing EU cybersecurity legislation[517]. In this respect, the NIS2 Proposal foresees the possibility for Member States to require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 (see section 3.5.3)[518].

Moreover, Article 54(3) CSA may offer insight into how the voluntary nature of cybersecurity certifications works in practice with EU cybersecurity legislation. Article 54(3) reads as follows: "where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act". A careful examination reveals this provision as an interface between *voluntary* schemes adopted under the Cybersecurity Act and *mandatory* requirements under other Union legal acts. Therefore, the Cybersecurity Act, while reversing the burden of proof, provides a legal basis for the alignment and harmonisation of *mandatory* requirements in EU cybersecurity legislation and *voluntary* certification schemes: even remaining voluntary, the ECCS may be used to comply with the mandatory requirements of other legal acts.

Certification is offered in principle by private entities which, in order to issue EU cybersecurity certificates, must be accredited by national accreditation bodies[519]. However, in duly justified cases, an ECCS may foresee that the certificates resulting from that scheme are to be issued only by a public body, namely the national cybersecurity certification authority or another public body. Said public entities must be accredited[520].

The risk-based approach[521] of the Cybersecurity Act is particularly reflected in the provision of granular and scalable 'assurance levels' ('basic', 'substantial' or 'high') that would provide the corresponding rigour and depth of the evaluation of the level of risk associated with the intended use of the ICT product, service or process[522]. Indeed, the scalability and granularity of the cybersecurity

[516] Regulation (EU) 2019/881, Recital 91.

[517] Regulation (EU) 2019/881, Recital 92.

[518] NIS2 Proposal, Art. 21(1)

[519] Regulation (EU) 2019/881, Article 60(1).

[520] Regulation (EU) 2019/881, Article 56(5)(b); Article 60(2).

[521] Mantelero and others (n 170).

[522] Regulation (EU) 2019/881, Article 52(1); Recital 86.

certification mechanisms may be better appreciated by considering who can issue which type of certificate and under which conditions.

With regard to the 'basic' assurance level only, the regulation allows manufacturers or providers of ICT products, services and processes that present a low risk – corresponding therefore to the lowest level – to perform a 'conformity self-assessment'[523], which must at least include a review of technical documentation[524]. This activity eventually results in an 'EU statement of conformity' demonstrating that the ECCS' requirements have been fulfilled[525].

Conversely, a European cybersecurity certificate that refers either to the 'substantial' or 'high' assurance levels cannot be issued by the manufacturer. The conformity assessment bodies will issue certificates referring to 'basic' and 'substantial' levels[526]. As regards the 'substantial' level, the evaluation activities must take into account the risk "carried out by actors with limited skills and resources" and shall include at least: (i) a review to demonstrate the absence of known vulnerabilities; and (ii) testing[527]. Any subsequently detected vulnerabilities or irregularities that could hinder compliance with the requirements related to the scheme must be notified by the holder of the certificate to the authority or the conformity assessment body[528]. This requirement is crucial since, paradoxically, certification – if obtained – may jeopardise its very own goals as a dynamic reality like cybersecurity could be falsely perceived as static. In other words, certification – if significant changes, such as subsequently discovered vulnerabilities, are not reported – "can make a product seem secure even if, after the trust mark is assigned, a serious security flaw is discovered"[529]. Depending on the type of update or patch, and in order to mitigate discovered vulnerabilities, cybersecurity re-certification of the component – or the whole system where the component is deployed – might be required. In turn, the cost of the re-certification process may constitute a hindrance to the regular production of updates and patches by manufacturers[530]. Thus, it has been estimated that the average cost of conformity assessment is in the range of €30.000-50.000 per company in a given year or

[523] Regulation (EU) 2019/881, Article 53(1).

[524] Regulation (EU) 2019/881, Article 52(5).

[525] Regulation (EU) 2019/881, Article 53(2).

[526] Regulation (EU) 2019/881, Article 56(4).

[527] Regulation (EU) 2019/881, Article 52(6).

[528] Regulation (EU) 2019/881, Article 56(8).

[529] Denardis (n 17) 119.

[530] Jose L Hernandez-Ramos, Sara N Matheu and Antonio Skarmeta, 'The Challenges of Software Cybersecurity Certification' (2021) 19 IEEE Security and Privacy 99, 101.

€3.000-4.000 per product basis[531]. Moreover, in the absence of quantitative and qualitative criteria that would set a threshold for the "skills and resources" of third parties (or attackers), such a *relativist* approach can prove to be troublesome to apply in practice.

Lastly, where a ECCS requires a 'high' assurance level, the certificate under that scheme is to be issued by a national cybersecurity certification authority or by a conformity assessment body if: (a) the national authority approves the issuing by conformity assessment bodies for each individual certificate; or (b) the national authority relies on a general delegation for the task of issuing such certificates to a conformity assessment body[532]. 'High' assurance levels will be evaluated to minimise the risk of state-of-the-art attacks carried out by actors with significant skills and resources. Compared to the requisites of the 'substantial' assurance level, the evaluation activities in this stage must also include an assessment of security functionality resistance through penetration testing[533], a cornerstone tool of cybersecurity[534].

With regard to enforcement powers, national authorities can carry out investigations (audits) of and take measures against certification bodies, certificate holders and issuers of EU statements of conformity to verify their compliance with Regulation 2019/881[535]. More importantly, they can require immediate cessation of infringements and impose penalties[536] according to the rules laid down by the Member States[537]. This decentralisation of an otherwise centralised legal framework may potentially lead, as noted by Kamara, "to a wide range of pecuniary penalties [and] undermine the guarantees to prevent forum-shopping offered by the common baseline rules"[538].

In conclusion, the EU cybersecurity certification legal framework, introduced by Regulation 2019/881, can arguably be seen as an important part of the Commission's ongoing programme in strengthen the Union's digital security. On the one hand, manufacturers, developers, vendors of ICT products, services and processes would rely on scalable and granular schemes to assess whether the specific security controls and measures of their technological solutions comply with specified security requirements. On the other hand, consumers and citizens will be offered information on the level of

---

[531] European Commission, 'COMMISSION STAFF WORKING DOCUMENT Part 1: Evaluation of the Internal Market Legislation for Industrial Products Accompanying the Document: The Communication from the Commission to the European Parliament, the Council and the European Economic and Social C' (2014) 66 <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52014SC0023> accessed 7 December 2021.

[532] Regulation (EU) 2019/881, Article 56(6).

[533] Regulation (EU) 2019/881, Article 52(7).

[534] Matt Bishop, 'About Penetration Testing' (2007) 5 IEEE Security and Privacy 84.

[535] Regulation (EU) 2019/881, Article 58(8) letters (b) and (c).

[536] Regulation (EU) 2019/881, Article 58(8)(f).

[537] Regulation (EU) 2019/881, Article 65.

[538] Kamara (n 465) 98.

security of certified ICT assets in a transparent manner. The inquiry revolved around the question of whether the Cybersecurity Act could eventually fill significant regulatory gaps and inconsistencies in the Union cybersecurity legal framework, in particular, regarding manufacturers and developers' lack of legal obligations vis-à-vis the cybersecurity of their technological solutions.

This section demonstrated that to consider the EU cybersecurity certification framework as *purely* voluntary is rather inaccurate. Thus, the legislator expressly left open the possibility of imposing specific cybersecurity requirements and making the certification thereof mandatory. Moreover, Member State law or other Union legal acts can provide for legally binding standards. In this respect, it has been highlighted that other EU legal acts may provide that a certificate (or an EU statement of conformity) adopted under the Cybersecurity Act may be used to demonstrate the presumption of conformity with requirements of those legal acts (for example, the essential requirements outlined in directives and regulations of the NLF, addressed in section 3.4). In this latter case, even if voluntary, certifications would be strictly linked with legally binding cybersecurity requirements. Notwithstanding the negative externalities arising from the high costs and low incentives[539], the ENISA conference on cybersecurity certification of 2-3 December 2021[540] stressed the key competitive advantage that comes with certification, as most of the customers and a significantly large part of the vendors of the supply chain look for certified products, services and processes, even if this costs them more[541]. In other words, market dynamics increasingly tend to make these private law instruments *de facto*, but not *de jure*, 'mandatory'.

[539] Wavestone - CEPS - CARSA - ICF, 'Study on the Need of Cybersecurity Requirements for ICT Products - No. 2020-0715: Final Study Report' (2021) 72 <https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products>.

[540] <https://www.enisa.europa.eu/news/enisa-news/going-full-throttle-on-cybersecurity-certification-and-market> accessed 3 December 2021.

[541] John M Blythe, Shane D Johnson and Matthew Manning, 'What Is Security Worth to Consumers? Investigating Willingness to Pay for Secure Internet of Things Devices' (2020) 9 Crime Science 1 <https://link.springer.com/articles/10.1186/s40163-019-0110-3> accessed 22 December 2021.

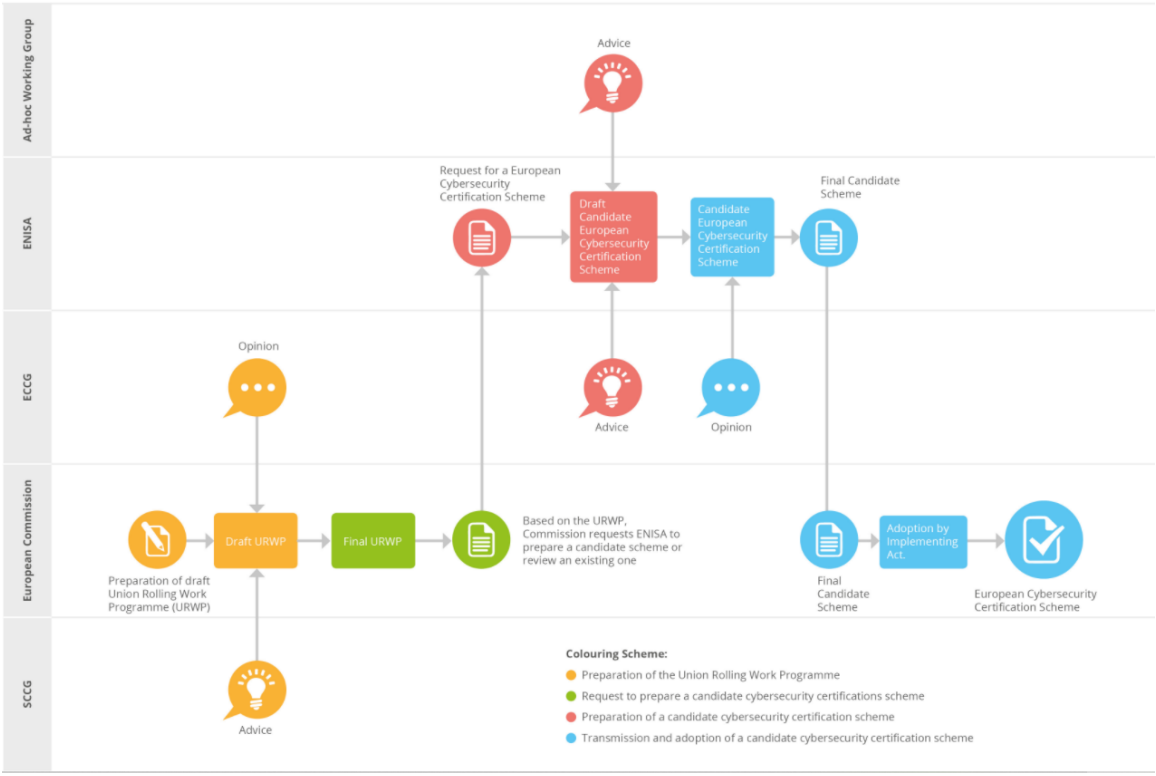


Figure 4: Stakeholders' interaction within the framework of the EU Cybersecurity Act[542]

3.3.2 The state of IoT cybersecurity certification and standardisation

The European Commission started to tackle the debate around the governance of IoT in 2012 by holding a multi-stakeholder public consultation[543]. Most respondents claimed that IoT-specific legislation, with respect to cybersecurity and safety, was not necessary, opting for no governance at all out of fear that overregulation coupled with unnecessary compliance burdens could stifle a fast-growing ecosystem still in its infancy[544]. Thus, there was a general consensus around the need for guidelines and standards, as a self-regulation governance approach was preferred. The initial pure self-regulatory policy option led to undesirable outcomes[545], namely an EU Internal Market flooded with unsecure IoT devices. Whereas the previous section demonstrated which actions the EU institutions have taken to put matters right (i.e., the adoption of Regulation 2019/881), this section

[542] <https://www.enisa.europa.eu/topics/standards/certification> accessed 7 December 2021.

[543] European Commission, *Conclusions of the Internet of Things Public Consultation* (2013) available at: <https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation> accessed 8 May 2021; Rolf H Weber, 'Internet of Things - Governance Quo Vadis?' (2013) 29 Computer Law & Security Review 341; Rolf H Weber, 'Governance of the Internet of Things—From Infancy to First Attempts of Implementation?' (2016) 5 Laws 28.

[544] Weber and Studer (n 394) 727.

[545] Luciano Floridi, 'The End of an Era: From Self-Regulation to Hard Law for the Digital Industry' (2021) 34 Philosophy & Technology 619.

aims at casting light on the plethora of technical standards, both European and national, on which existing IoT cybersecurity labels and future certification schemes will be based.

Against the background of the IoT governance debate, some scholars argued that "we lack the proper technical standards that may enable multiple systems and different networks to communicate with each other, making full interoperability feasible"[546]. Interestingly, the lack of interoperable solutions and upstream technical standards is echoed in Recital 66 of the Cybersecurity Act, warning that such gaps – coupled with missing practices and Union-wide mechanisms of certification – significantly affect the single market in the field of cybersecurity[547]. The lack of interoperability is certainly the thorniest obstacle that may still hinder the IoT from its full realisation: as stressed by the EU Commission's 2019 Rolling Plan for ICT standardisation, after the adoption of the Cybersecurity Act, "[i]nteroperability between IoT networks operated by different companies along the value chain opens up opportunities to address EU policy objectives e.g., greater resource efficiency for a more circular economy, sustainable and responsible supply chains through transparency and traceability, and others"[548].

There is nevertheless an argument against the push for interoperability that deserves attention. Denardis notes that a certain degree of lack of interoperability could be at times beneficial in the IoT cybersecurity paradigm:

> *"Designing a medical monitoring device to communicate directly with a door lock is both unnecessary and undesirable, especially from a security standpoint. Having some inherent lack of interoperability between different implementation settings, particularly by sector, assuming each environment itself develops sufficient stability and security, seems preferable to a wide-open plane of attack for cross-sector and cross-border security incursions"*[549].

The argument made above may be better grasped through an example, namely the role Android played for smartphones. Before Android, there were many 'little islands' of non-interoperable phones (e.g., Nokia, Samsung, LG, etc.). As a consequence, different apps had to be developed for each 'type of island'. With the advent of Android, most devices in the world (except Apple's) have become interoperable with each other. On the one hand, it is true that this process has created a single point of failure, that is, an exploit for Android would endanger millions of devices. On the other hand,

---

[546] Pagallo, Durante and Monteleone (n 77) 74.

[547] Regulation (EU) 2019/881, recital 66.

[548] European Commission, 'Rolling Plan for ICT Standardisation 2019' (2019) 25.

[549] Denardis (n 17) 136.

different sectors – medical devices and door locks – have different standards: to ensure interoperability in a single environment, it is necessary to have a higher standard that would link the sectorial standards at the lower level. Beside the fact that security is always a central element in the standardisation process, sectorial fragmentation – while potentially representing a barrier to standardisation[550] – is crucial to uphold cybersecurity, as indeed highlighted, to a certain extent, by Denardis: "fragmentation by industry might be desirable so that […] a lack of cross-industry interoperability can serve as a check on security problems"[551]. To conclude, a medical IoT device and a door lock might well interoperate in some way (even without any useful purpose), but they would still not be considered 'equal devices' when communicating because of the different (sectoral) standards, thus ensuring a desirable degree of security.

Nevertheless, in the 2021 Rolling Plan, the Commission noticed that "a large number of proprietary or semi-closed solutions to address specific problems have emerged, leading to non-interoperable concepts, based on different architectures and protocols. Consequently, the deployment of truly IoT applications i.e., where information of connectable "things" can be flexibly aggregated and scaled, has been limited to a set of "intranets of things — or goods"[552]. In this respect, it is worth recalling the IoT architecture taxonomy outlined in Chapter 1, as the strive for standards for these systems goes beyond the end devices – which are mostly constrained[553] – and involves communication networks, switching and routing systems, back-end analytics, applications, cloud services. Therefore, it extends to a plethora of different markets, business models and actors. On the other hand, the Commission acknowledges that one of the major achievements of the last few years has been the progressive strength of cooperation amongst all actors in the field of IoT standardisation[554] to develop common technical standards, eschewing the path towards proprietary approaches. Against this backdrop, the question that arises is what the state of IoT standardisation in the specific area of security is.

At the end of 2018, ENISA conducted a preliminary analysis of the IoT-related landscape of security standards[555]. The model consists of mapping cybersecurity requirements to available standards, from European Standardisation Organisations (i.e., CEN, CENELEC and in particular ETSI TC Cyber), ISO/IEC JTC1 subcommittees including SC27 (IT Security Techniques) and SC41 (Internet of

[550] ibid 142.

[551] ibid 144.

[552] European Commission, 'Rolling Plan for ICT Standardisation 2021' (n 2) 30.

[553] There are many standards and protocols for IoT constrained scenarios: CoAP, IPv6 over Bluetooth, LoRAWAN, DDS, DTLS, ZigBee, etc.

[554] European Commission, 'Rolling Plan for ICT Standardisation 2021' (n 2) 31.

[555] ENISA, 'IoT Security Standards Gap Analysis: Mapping of Existing Standards against Requirements on Security and Privacy in the Area of IoT' (2019).

Things and related technologies) and ITU-T Series Y: "Global information infrastructure, internet protocol aspects and next-generation network". The multiple requirements identified by Annex I of the matrix are clustered around several classes. These are: 'security by design', 'privacy by design', 'organisational, people and process measures'[556].

The Agency came to the conclusion that "there is no significant gap in standards to bring secure IoT to the market. This does not mean that the security of the IoT ecosystem as a whole has been addressed by means of standards. Elements of a holistic approach towards IoT security can be found in a series of standards, however, to achieve an overarching approach that protects the entire IoT ecosystem further work is needed"[557]. In other words, what is really lacking in IoT security standardisation is a *functional* – that is, sector and application (products, services or processes) specific, *flexible*, *holistic* combination of the technical requirements that already exist out there. As a consequence, it is possible "to deliver a device to the market that can authenticate its user, that can encrypt data it transmits, that can decrypt data it receives, that can deliver or verify the proof of integrity, but which will still be insecure"[558].

Amongst the many standards mapped out by ENISA, it is worth looking more closely at ETSI's Cybersecurity standard for Consumer IoT (ETSI EN 303 645) and ISO/IEC's IoT security and privacy (ISO/IEC CD 27402) standards. Indeed, they are mentioned by experts as a good basis for the development of harmonised standards for baseline cybersecurity of connected products[559]. Whereas ISO/IEC 27402 (*Cybersecurity — IoT security and privacy — Device baseline requirements*) is currently under development[560], in 2020 ETSI released a standard which specifies 13 cybersecurity baseline requirements for consumer IoT devices, with specific considerations to constrained devices[561] (see Chapter 1), with the associated services being out of the scope[562]. The cybersecurity baseline requirements are:

---

[556] ibid 11–22.

[557] ibid 4.

[558] ibid 7.

[559] DIGITALEUROPE, 'Setting the Standard: How to Secure the Internet of Things' (2021) 15 <https://www.digitaleurope.org/wp/wp-content/uploads/2021/07/DIGITALEUROPE_Joint-> accessed 18 October 2021.

[560] The standard proposal was approved in mid-June 2020. See <https://www.iso.org/standard/80136.html> accessed 14 December 2021.

[561] ETSI defines it as a "devices which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use".

[562] ETSI, 'EN 303 645 V2.1.1 - Cyber Security for Consumer Internet of Things: Baseline Requirements' (2020) 6.

(i) No universal default passwords: the passwords shall be unique per device and sufficiently randomized to reduce the risk of automated attacks (provisions 5.1-1,2). Moreover, authentication mechanisms shall use state-of-the-art cryptography (provision 5.1-3).

(ii) Implement a means to manage reports of vulnerabilities: the manufacturer shall render publicly available a vulnerability disclosure policy, including contact information for the reporting and information on timelines vis-à-vis the acknowledgment of receipt and status updates (provision 5.2-1). In this regard, the manufacturer should act on vulnerabilities in a timely manner without stopping the continuous monitoring (provisions 5.2-2,3).

(iii) Keep software update: all software components shall be securely updatable (provision 5.3-1) and the process will be simple (provision 5.3-3), automated (provision 5.3-4) – even if the update would involve dependencies on multiple actors along the supply chain and possibly separated from feature updates. The device should verify authenticity and integrity of software updates: in resource constrained paradigms, verification can be performed by a trusted device (provision 5.3-9). If a constrained device cannot have its software updated, it should be isolable (provision 5.3-15) and the manufacturer should publish the reasons for this, alongside the period and method of hardware's replacement provision (5.3-14). Finally, the manufacturer should inform users whether a security update is required, and how the risks have been mitigated (provision 5.3-11).

(iv) Securely store sensitive security parameters: security parameters like hard-coded unique identity shall be implemented in a way that resists tampering (provision 5.4-2).

(v) Communicate securely: device shall use best practice cryptography and state-of-the-art implementations to deliver network and security functionalities (provisions 5.5-1, 2).

(vi) Minimize exposed attack surfaces: the foundational 'principle of least privilege' shall be taken into the utmost account. As a consequence, software should run with the lowest possible number of privileges (provision 5.6-7), unused network and logical interfaces shall be disabled (provision 5.6-1) and, when in the initialized state, the former shall minimise the unauthenticated disclosure of security-relevant information (provision 5.6-2). If a debug interface is physically accessible, it shall be disabled in software (provision 5.6-4). Finally, the manufacturer should follow secure software development processes (provision 5.6-9)[563].

(vii) Ensure software integrity: software should be verified through secure boot mechanisms (provision 5.7-1) and if unauthorised change is detected, the device should alert the user and/or the administrator (provision 5.7-2).

[563] ENISA, 'Good Practices for Security of IoT Secure Software Development Lifecycle' (n 451).

(viii) Ensure that personal data is secure: this control upholds confidentiality of personal data, especially taking into account the ones transiting between a device and a service. Interestingly, ETSI provides for a definition of 'sensitive personal data' in "note 1" of the provision 5.8-2 which diverges to a certain extent from the GDPR approach: whereas the (exceptional) grounds for the processing of 'special categories of personal data'[564], that is, "sensitive data", laid down by Regulation (EU) 2016/679 are set in relationship to significant risks to the fundamental rights and freedoms[565], ETSI conceives 'sensitive data' as data whose disclosure has a high potential to cause harm to the individual.

(ix) Make systems resilient to outages: *resilience by design*, that is, building devices taking into account the eventuality of power and network outages (provision 5.9-1): in case of a loss of network access the IoT device should remain operating (provision 5.9-2). Redundancy and mitigations against DDoS attacks should be included as well.

(x) Examine system telemetry data for security anomalies

(xi) Make it easy for users to delete user data: user data shall be deleted from the device (provision 5.11-1) as well as from associated services (provision 5.11-2) in a simple manner. In this respect, users should be given clear instructions on how to do so (provision 5.11-3) and provided with confirmation about whether cancellation has been successful (provision 5.11-4).

(xii) Make installation and maintenance of devices easy: these steps should involve minimal decisions by the user (provision 5.12-1) and the manufacturer should provide users with sufficiently clear guidance on how to securely set up the device (provision 5.12-2) and how to check whether the previous step has been achieved (provision 5.12-3).

(xiii) Validate input data via user interfaces or transferred via APIs or between networks in services and devices (provision 5.13-1)[566].

[564] Regulation (EU) 2016/679, Article 9.

[565] Regulation (EU) 2016/679, Recital 51.

[566] ETSI (n 562) 13–24.

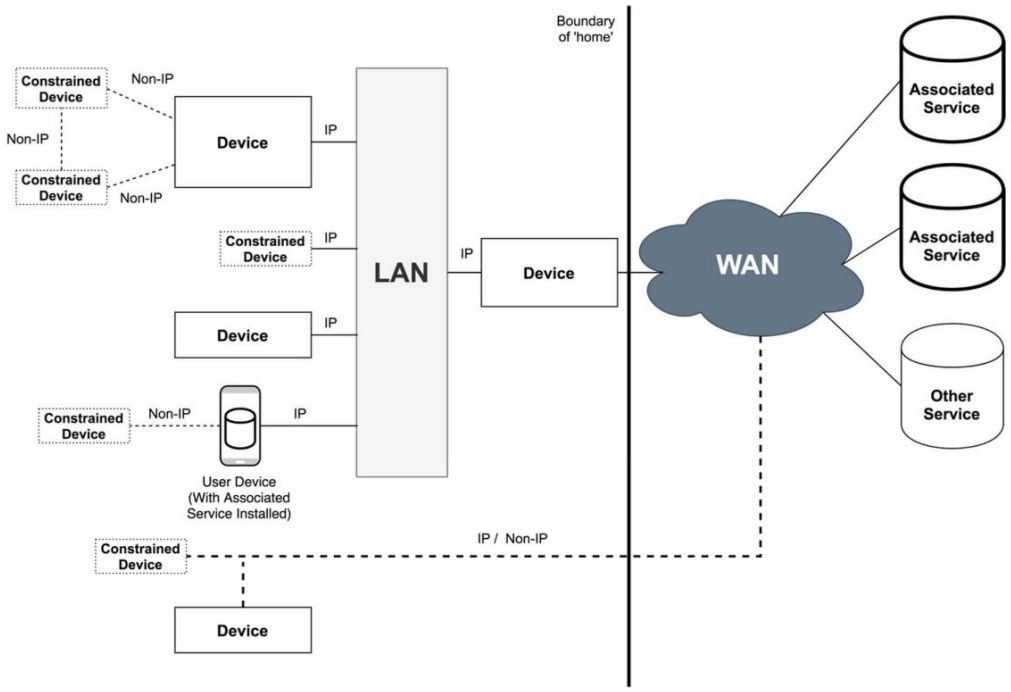


Figure 5: Example of a reference architecture for consumer IoT deployment in a domestic environment[567]

In light of the above, it can be argued that numerous efforts have been made with respect to IoT security standardisation. In this respect, ENISA's mapping out of security standards applicable to IoT shows that "there is a gap in standards only insofar as it is unclear what combination of standards, when applied to a product, service or system, will result in a recognisably secure IoT"[568]. However, it should be noted that technical experts agree that existing and soon-to-be-published standards, that is, ETSI TS 303 645 and ISO/IEC 27402, would only cover roughly half (54%) of the technical requirements that can be used as harmonised standards based on current product legislation[569]. Further work is therefore necessary in order to define baseline cybersecurity requirements for all IoT connected devices that would be referenced in harmonised standards under EU product legislation, which will be addressed subsequently in section 3.5.

Based on the requirements of ETSI TS 303 645, the Finnish Transport and Communications Agency (Traficom) has created a Cybersecurity Label, which is, a certification scheme for IoT devices or services[570]. The Finnish label extends ETSI's baseline cybersecurity requirements from 13 to 20 and prioritises them according the OWASP IoT threats list in order to encompass the most common

[567] ibid 27.

[568] ENISA, 'IoT Security Standards Gap Analysis: Mapping of Existing Standards against Requirements on Security and Privacy in the Area of IoT' (n 555) 23.

[569] DIGITALEUROPE, 'Setting the Standard: How to Secure the Internet of Things' (n 559) 15.

[570] Finnish Transport and Communications Agency, 'Finnish Cybersecurity Label' (2020) <https://tietoturvamerkki.fi/files/cybersecurity_label_presentation-280920.pdf>.

security threats affecting the consumers of connected devices[571]. Moreover, from an operational viewpoint, the Label shows how the relationship between certification (even though it has not been developed under the Cybersecurity Act framework) and standards upon which the former rely on works in practice. Following the Swedish lead, on 27 September 2022, the German Federal Office for Information Security (BSI) released an IT security label for IoT consumer devices, building on the EU cybersecurity standard for IoT consumer devices ETSI EN 303 645[572].

Isolated national cybersecurity certification initiatives in the IoT sector (such as the Finnish and German IoT security labels) may even achieve their objectives and prove useful in the short term. They run the risk, however, of further fragmenting the EU cybersecurity certification landscape. The Cybersecurity Act, as shown in this Chapter, aims to tackle the current fragmentation of the internal market with harmonised European Cybersecurity Certification Schemes.

Against this backdrop, the Rolling Plan of the EU Commission does not foresee a cybersecurity certification scheme directly addressing the IoT. Instead, the Commission focused on the need of technical security standards for the IoT and proposed as a priority action the development of a European standard for cybersecurity compliance of products that is aligned with the current information security compliance framework of ISO 27000's family and the GDPR. On the other hand, the standard will be used to harmonise the requirements set out in the NIS directive[573]. As Chapter 5 will later discuss vis-à-vis risk analysis frameworks, the need is to correctly position EU core values and principles in IoT standardisation regarding existing global initiatives such as the ones of ISO/IEC. Moreover, EU standardisation organisations are required to fill further gaps and develop standards on the safety and cybersecurity of IoT consumer products under the European Cybersecurity Act or sectorial legislation e.g., the NLF[574].

While awaiting a future candidate IoT scheme[575], three candidate schemes are under development: the first and more advanced EU Cybersecurity Certification Scheme on Common Criteria (EUCC)[576] – which may serve as a successor to the EU national schemes operating under the SOG-IS MRA, the

---

[571] ibid 14.

[572] German Federal Office for Information Security (BSI), 'IT Security Label for All "Smart Consumer Devices"' (2022) <https://www.bsi.bund.de/SharedDocs/IT-Sicherheitskennzeichen/DE/Meldungen/Smarte-Verbrauchergeraete.html>.

[573] European Commission, 'Rolling Plan for ICT Standardisation 2021' (n 2) 32.

[574] ibid.

[575] ENISA Stakeholder Cybersecurity Certification Group, 'Consultation Report on Draft URWP' (2021) 10–13.

[576] ENISA, 'Public Consultation on the Draft Candidate EUCC Scheme' (2021); ENISA, 'Cybersecurity Certification: Candidate EUCC Scheme V1.1.1' (2021).

EU Cybersecurity Certification Scheme on Cloud Services (EUCS)[577] and the one on 5G[578]. In particular, the EUCC is more of a horizontal scheme: "it may allow to improve the Internal Market conditions, and to enhance the level of security of ICT products dedicated to security (e.g., firewalls, encryption devices, gateways, electronic signature devices, means of identification such as passports, …) as well as of any ICT product embedding a security functionality (i.e., routers, smartphones, banking cards, medical devices, tachographs for lorries, …)"[579]. As such, IoT manufacturers and developers may consider certifying some ICT products embedded in their IoT solutions. This paradigm has been identified as 'certification by composition': an IoT device may rely on certified components (e.g., firewalls) thanks to the EUCC and on a certified cloud service, thanks to the EUCS[580]. In conclusion, a future candidate IoT security scheme should attempt to exploit synergies between existing labels and schemes.

3.4 The Revision of EU Product Legislation and its Interplay with IoT Cybersecurity

3.4.1 Introducing cybersecurity essential requirements in new legislative framework directives

The entry into force of the so-called 'New Legislative Framework' (NLF) in 2008 marked the start of a new approach in the European model of governance of product safety. The NLF consists of Regulation (EC) 765/2008, setting out the requirements for accreditation and the market surveillance of products; Decision 768/2008 on a common framework for the marketing of products, which includes reference provisions to be incorporated whenever product legislation is revised; and, Regulation (EU) 2019/1020 on market surveillance and product compliance.

The New Legislative Framework updated the foundational principles of the 'New Approach', developed in the 80s as a legislative follow-up to the *Cassis de Dijon* seminal case[581], towards technical harmonisation in the context of EU products safety legislation[582]. The 'New Approach' model of governance pivoted around four core principles. First, legislative harmonisation should be

[577] ENISA, 'EUCS - CLOUD SERVICES SCHEME: EUCS, a Candidate Cybersecurity Certification Scheme for Cloud Services' (2020).

[578] See <https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification> accessed 18 December 2021.

[579] ENISA, 'Cybersecurity Certification: Candidate EUCC Scheme V1.1.1' (n 576) 11.

[580] ECSO, 'European Cyber Security Certification - Challenges Ahead for the Roll-out of the Cybersecurity' 15 <https://ecs-org.eu/documents/publications/5fd787e5cae1c.pdf>.

[581] Case 120/78, *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein* (Cassis de Dijon) [1979] EU:C:1979:42.

[582] Hofmann (n 469) 17.

limited to lay down the 'essential requirements' (ERs) – as opposed to overly detailed technical proscriptions that products placed on the EU market must meet in order to benefit from free movement within the EU[583]. Second, European Standardisation Organisations (ESOs) i.e., CEN, CENELEC and ETSI, shall be mandated by the Commission with the task of establishing specific technical standards – known as 'harmonised technical standards' – for products meeting the essential requirements set out in the legal acts[584]. Third, products manufactured in compliance with harmonised standards benefit from a presumption of conformity with the corresponding essential requirements of the applicable legislation. Fourth, the application of harmonised or other standards remains voluntary, and the manufacturer can always apply other technical specifications to meet the requirements[585].

The NLF updated EU legislation with a more comprehensive and coherent regulatory framework in relation to market access (that is, notification process, accreditation, the conformity assessment procedures, CE marking) and market surveillance. The emphasis shifts from the traditional notion of 'placing on the market' – which focuses on the first time a product is made available on the EU market, to 'making a product available'[586]: the latter concept, while giving more importance to what happens after a product is first made available, facilitates the tracing back of a noncompliant product to the manufacturer[587]. This approach is further complemented by putting in place a comprehensive policy on market surveillance, that is, Regulation (EC) no. 765/2008 and Regulation (EU) 2019/1020. "This has considerably changed the balance of EU legislative provisions from being fundamentally oriented at setting product related requirements to be met when products are placed on the market to an equal emphasis on enforcement aspects during the whole life-cycle of products"[588].

---

[583] Lukasz Gorywoda, 'The New European Legislative Framework for the Marketing of Goods' (2009) 16 Columbia Journal of European Law 161, 163.

[584] In this respect, such delegation – either via contracts or not – raised a question of the constitutional legitimacy, in terms of the principles of access and transparency, of referencing (EU) harmonised technical standards or ISO standards in EU law without publishing their content in the Official Journal of the EU: see *ex multis* Marie Gérardy, 'Nemo Censetur Ignorare Legem: The Dilemma Regarding the Access to ISO Standards Referenced into EU Law' (*REALaw.blog*) <https://realaw.blog/2021/11/23/nemo-censetur-ignorare-lege-the-dilemma-regarding-the-access-to-iso-standards-referenced-into-eu-law-by-marie-gerardy/> accessed 7 December 2021. Albeit extremely interesting, the legal qualification of harmonised technical standards and the possibility of their undergoing judicial verification of their validity under EU law fall outside the scope of this work; see *inter alia*, Gabriella Perotto, 'La Standardizzazione Europea Nel Settore Dell'ICT Nell'era Dell'Internet of Things: Qualificazione Giuridica e Controllo Di Validità Degli Standard Tecnici Armonizzati ' (2020) 3 Il diritto dell'economia 757.; CJEU Case C-613/14, *James Elliott Construction Limited c. Irish Asphalt Limited* [2016] ECLI:EU:C:2016:821.

[585] European Commission, 'The "Blue Guide" on the Implementation of EU Products Rules 2016 (2016/C 272/01)' [2016] Official Journal of the European Union 8 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016XC0726(02)&from=EN%0Ahttp://ec.europa.eu/DocsRoom/documents/18027/>.

[586] On the difference between 'placing on the market' and 'making available on the market', see Decision No 768/2008/EC, Annex I, Article R1(1), (2) and Regulation (EC) No 765/2008, Article 2(1), (2).

[587] European Commission, 'The "Blue Guide" on the Implementation of EU Products Rules 2016 (2016/C 272/01)' (n 585) 10.

[588] ibid.

Against this background, most of the legal acts in the area of EU product legislation, and the related harmonised standards which specify the ER thereof, were conceived before the advent of the IoT; in other words, when products were not connected and did not interact with each other or their environment[589]. Therefore, the EU Commission aims at leveraging the EU product safety legal frameworks by including cybersecurity essential requirements in the revision process of different legislative pieces[590]. Thus, the Commission deemed it reasonable to firstly tackle the issue of unsecure connected products from a sectorial, or vertical, viewpoint rather than embarking on a long legislative process in view of the introduction of a horizontal piece of legislation on cybersecurity[591].

This section critically analyses the EU legal frameworks regulating product safety to assess to what extent the cybersecurity of (IoT) products is considered. One methodological caveat applies. Considerations on safety requirements generally involve the analysis of civil – or even criminal – liability regimes[592]. Nevertheless, liability issues fall outside the scope of this thesis[593]. Yet, this section delves into different legal acts of EU product legislation only to the extent that they incorporate cybersecurity essential requirements applicable to the IoT. Building on the theoretical premise of section 2.2.4 ("*Degrees of Separation Between Cybersecurity and Safety in the IoT*"), this legal analysis casts light on how the EU co-legislator envisages the entanglement of the concepts of safety and cybersecurity with regard to the IoT devices[594].

The first Directive under scrutiny is Directive 2014/53/EU on radio equipment[595] which, needless to say, is particularly prominent in the context of the IoT ubiquitous connectivity. The Proposal for a Regulation on General Product Safety[596] would introduce a cybersecurity requirement that would be taken into account when assessing the safety of (connected) products, including therefore IoT.

---

[589] Eduard Fosch-Villaronga and Tobias Mahler, 'Cybersecurity, Safety and Robots: Strengthening the Link between Cybersecurity and Safety in the Context of Care Robots' (2021) 41 Computer Law & Security Review, 6.

[590] DIGITALEUROPE, 'Setting the Standard: How to Secure the Internet of Things' (n 559) 4.

[591] COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29.10.2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive, 5.

[592] European Commission Expert Group on Liability and New Technologies (n 441).

[593] See *ex multis* Chiara, 'Sistemi Intelligenti Autonomi e Responsabilità Civile: Stato Dell'arte e Prospettive Nell'esperienza Comunitaria' (n 442).

[594] Vedder (n 304) 14–15; Wolf and Serpanos (n 305); Pier Giorgio Chiara, 'The Balance Between Security, Privacy and Data Protection in IoT Data Sharing: A Critique to Traditional "Security&Privacy" Surveys' (2021) 7 European Data Protection Law Review 18.

[595] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance.

[596] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council
COM/2021/346 final

Moreover, the Medical Devices Regulation (MDR) is considered as it is the first EU legal act, with an impact on a specific IoT sector (i.e., e-Health), that incorporated cybersecurity requirements. Finally, the Proposal for a Regulation on Machinery Products[597], repealing Directive 46/2002/EC, would lay down cybersecurity requirements for the design and construction of machinery products[598].

3.4.2 The Radio Equipment Directive (RED) and the Delegated Act

Directive 2014/53/EU on radio equipment (RED)[599] establishes a regulatory framework for the making available of radio equipment on the EU market[600]. The RED aligned the previous directive, the radio and telecommunication terminal equipment directive (1999/5/EC) with the New Legislative Framework principles for the marketing of products and for improved market surveillance. In particular, an efficient traceability system pivoting on the identification of radio equipment is foreseen in the 'EU declaration of conformity'[601] – issued by the manufacturer – in order to facilitate market surveillance authorities' task of tracing economic operators (i.e., manufacturers, importers and distributors) who made non-compliant radio equipment available on the market[602]. Improved market surveillance is also testified by the manufacturers' obligation to register radio equipment falling within categories affected by a low level of compliance with the essential requirements set out in Article 3 in a central system made available by the Commission before market placement[603].

Article 3 lays down the 'essential requirements' (ER) radio equipment must comply with[604]. Importantly, Article 44 empowers the Commission to adopt delegated acts to specify which categories or classes of radio equipment are concerned by each of the safety requirements laid down in Article 3(3)[605]. Among the nine ERs listed in Article 3(3), for the purpose of this work, it is worth focusing

---

[597] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on machinery products" COM(2021) 202 final.

[598] Essential Health and Safety Requirements (EHSR) in Annex III will be modified to address cybersecurity issue with an impact on safety: i) EHSR 1.1.9: security by design of machinery products; ii) EHSR 1.2.1: security by design of control systems.

[599] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance.

[600] Directive 2014/53/EU, Article 1(1).

[601] Directive 2014/53/EU, Annex IV.

[602] Directive 2014/53/EU, Recital 37.

[603] Directive 2014/53/EU, Article 5(1).

[604] Pursuant to Article 17(2), manufacturers shall demonstrate compliance of radio equipment with the essential requirements set out in Article 3(1) using any of the following conformity assessment procedures: (a) internal production control set out in Annex II; (b) EU-type examination that is followed by the conformity to type based on internal production control set out in Annex III; (c) conformity based on full quality assurance set out in Annex IV.

[605] Directive 2014/53/EU, Article 44; 3(3).

on Article 3(3)(d)[606], (e)[607] and (f)[608], namely the ERs that aim to address different elements of cybersecurity by ensuring network protection, safeguards for the protection of personal data and privacy, and, protection from fraud respectively.

As to the question whether IoT devices fall under the scope of the RED, Directive 2014/53 defines 'radio equipment' as an "electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication"[609]. Therefore, if an IoT device communicate via radio-based protocols such as Bluetooth (indirect internet-connectivity) or Wi-Fi (direct internet-connectivity), it would be radio equipment within the meaning of Article 2(1) RED[610]. The Impact Assessment on the increased protection of internet-connected radio equipment and wearable radio equipment commissioned by the Commission from the *Centre for Strategy & Evaluation Services* came to the same conclusion[611].

Since radio equipment is increasingly connected to the internet (the number is estimated to rise to 7.43 billion in EU by 2030), concerns are arising as to whether these devices – including machines, sensors and networks that make up the Internet of Things (IoT) – are sufficiently secure (as seen in Chapter 1) to ensure that users personal data and networks are protected, privacy is respected and frauds are avoided[612]. In 2019, the Commission started a public consultation taking into account all the possible related aspects, "also in terms of the impacts for the society (e.g. consumers and economic operators), the national Authorities, the common market access conditions and the implementation of, or synergies with, additional pieces of EU legislation, in particular those relating to (cyber)security, data protection and privacy"[613]. Thus, the already existing pieces of EU legislation

---

[606] Article 3(3)(d) mandates that radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.

[607] Article 3(3)(e) prescribes that radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.

[608] Article 3(3)(f) requires that radio equipment supports certain features ensuring protection from fraud.

[609] Directive 2014/53/EU, Article 2(1)(1).

[610] Hessel and Rebmann (n 25), 34.

[611] Center for Strategy & Evaluation Services, 'Final Report: Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment' (2020) 13 <https://ec.europa.eu/docsroom/documents/40763>.

[612] ibid 14; Chiara Giovanni and Frederico Silva, 'Cybersecurity for Connected Products - ANEC BEUC Position Paper' (2018) 4. See also <https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/b4016779-5e33-4298-b64e-a2cce6f4dba2/details> accessed 24 January 2022; <https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/ffef4de7-cbc0-4f78-968b-2b6b355d5aec/details> accessed 24 January 2022; OECD, 'Consumer Product Safety in the Internet of Things' (2018) 267 OECD DIGITAL ECONOMY PAPERS, 18 and ff.

[613] European Commission, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Commission Delegated Regulation Supplementing Directive 2014/53/EU of the European Parliament and of the Council with Regard to the Application of the Essential Requireme' (2021) Annex II, 62 <https://ec.europa.eu/growth/system/files/2021-10/SWD%282021%29 302_EN_impact_assessment_part1_v3.pdf>.

regulating privacy, data protection, frauds or networks security (i.e., GDPR, ePrivacy Directive, NIS Directive and Non-Cash Payment Directive) do not allow effective corrective measures to be taken in terms of withdrawal against insecure connected products that are placed on the market. Against this background, the delegated act activating the essential requirements under Article 3(3)(d), (e) and (f) RED would oblige manufacturers to design the equipment in a more secure manner as a pre-condition for market access.

Thus, under the RED's essential requirements, the competent authorities of the Member States cannot remove IoT products from the market if they fail to comply with the relevant legislation (e.g., the GDPR, the e-Privacy Directive or the incoming ePrivacy Regulation, which would include machine-to-machine communications), unless the delegated act is adopted[614]. Secondly, in the early stages of a product's design and engineering, if there is no intention to collect any personal data, the manufacturer is not obliged to consider, *inter alia*, data protection by design and by default principles or, more generally, the whole GDPR[615]. In this scenario, the inherent risk is the potential overlooking of GDPR's security considerations, as the allegedly non-personal data being processed could wrongly justify a lower standard of protection. To make things more complex, it is very likely that the opposite scenario will occur i.e., where an IoT device generates personal data, pursuant to the definition of Article 4(1) GDPR and the identifiability test of Recital 26[616], and relevant case-law[617], which is then subsequently collected and shared with third parties such as cloud service providers.

The Commission eventually adopted the delegated regulation on 29 October 2021[618]. As mentioned above, the objective of the delegated act is to specify to which categories or classes of radio equipment the essential requirements set out in Article 3(3)(d), (e) and (f) of the RED apply.

Whereas Article 3(3)(e) is yet another interface in which we can better appreciate the common approach of EU regulation vis-à-vis cybersecurity and data protection[619], provided that an artificial

---

[614] CSES, "Final Report - Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment" (2020), 96.

[615] ibid, 35.

[616] Michèle Finck and Frank Pallas, 'They Who Must Not Be Identified — Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 International Data Privacy Law 11, 11.

[617] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779; Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994.

[618] Commission Delegated Regulation (EU) 2022/30 of 29.10.2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive.

[619] European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy (n 15), 4.

distinction between these realms only leads to detrimental effects[620], Article 3(3)(d) directly concerns 'cybersecurity' as radio equipment that will have to incorporate features, that is, cybersecurity measures or controls, to avoid harm, the functioning nor misuse of networks and network resources. As clarified by Recital 9 of the Delegated Act, the 'network security' requirement should be interpreted broadly to cover main cybersecurity threats[621], such as DDoS attacks[622]. The rationale underpinning an 'absolutist' understanding of "harm to network" is to be found in the more complex, extensive and dynamic threat landscape – with 5G being a major driver of such expansion of threat vectors[623]. Therefore, Article 3(3)(d) would not only take into account the 'proper' use that radio equipment make of the network but also the harmful consequences to the network arising from insufficient security, that is, insufficient authentication, against cyberattacks[624]. In other words, the delegated regulation would complement the framework established by the NIS Directive, ensuring that not only the networks *per se* are secure, but also that the connected radio equipment does not harm them[625].

With the adoption of the delegated act, the 'network-preservation' requirement of Article 3(3)(d) will apply to radio equipment that communicates *directly* and *indirectly* – i.e. via other equipment (e.g., Bluetooth and other similar protocols which may enable wireless data sharing with internet-connected equipment) – over the internet[626]. Conversely, the privacy and data protection requirement (Article 3(3)(e)) is also applicable to radio equipment designed or intended exclusively for childcare, toys and 'wearables'[627]. The reference to 'toys' is not trivial, as the notorious case of the *Cayla* doll[628] showed

---

[620] Alessandro Mantelero, Giuseppe Vaciago, Maria Samantha Esposito and Nicole Monte, "The common EU approach to personal data and cybersecurity regulation" (2021) International Journal of Law and Information Technology, Oxford University Press, 2.

[621] RED delegated act, recital 9: "an attacker may maliciously flood the internet network to prevent legitimate network traffic, disrupt the connections between two radio products, thus preventing access to a service, prevent a particular person from accessing a service".

[622] *Contra* see Cezary Banasinski and Marcin Rojszczak, 'Cybersecurity of Consumer Products against the Background of the EU Model of Cyberspace Protection' (2021) 00 Journal of Cybersecurity 1, 7.

[623] ENISA, 'ENISA Threat Landscape for 5G Networks' (n 118).

[624] European Commission, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Commission Delegated Regulation Supplementing Directive 2014/53/EU of the European Parliament and of the Council with Regard to the Application of the Essential Requireme' (n 613) 12–17.

[625] ibid 5.

[626] RED delegated act, Article 1(1).

[627] RED delegated act, Article 1(2).

[628] Steve Mansfield-Devine, 'Weaponising the Internet of Things' (2017) 2017 Network Security 13.

that national Market Surveillance Authorities[629] found it difficult to remove the product from the market, even though various security flaws and vulnerabilities had been exposed[630].

Finally, Article 2 of the delegated act derogates from Article 1 by excluding medical and in-vitro devices from the scope of all the RED essential requirements[631], whilst motor vehicles, electronic road toll systems, equipment to control unmanned aircraft remotely as well as non-airborne specific radio equipment that may be installed on aircrafts are exempt from the requirements regarding the protection of personal data and protection against fraud[632]. Thus, the cybersecurity requirement of Article 3(3)(d) against networks harm and misuse would still be applicable to these legislations.

The recently adopted delegated act brings the majority of IoT devices into the RED's scope, albeit the RE already on the market when the delegated regulation entered into force are not addressed. Despite the scope of the RED being limited to wireless, thus leaving out wired devices, the adoption of the delegated act would indeed enhance and complement the existing standards of protection under cybersecurity and data protection EU legislation, with the key objective being to strengthen the 'ecosystem of trust' which stems from the synergies of all related pieces of EU law concerning protection of networks, privacy and against fraud[633]. All manufacturers of internet-connected and wearable devices must therefore design products that embed baseline (cyber)security and data protection requirements as a pre-condition for market access, even if they claim not to process personal data[634]. Under the RED, security and data protection by design would become a condition of market access[635]: as a result, national competent authorities – if provided by Member States with adequate powers and resources vis-à-vis the supervision of consumer products' cybersecurity – will be able to remove non-compliant products from the market.

Following the adoption of the delegated act(s), the European Commission will issue a standardisation mandate to the ESOs. In line with the New Legislative Approach principles, these stakeholders will

---

[629] Germany resorted to a longstanding legal act on espionage to remove the product on the market; See <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html?nn=690686> accessed 25 January 2022.

[630] European Commission, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Commission Delegated Regulation Supplementing Directive 2014/53/EU of the European Parliament and of the Council with Regard to the Application of the Essential Requireme' (n 613) 27.

[631] RED delegated act, Article 2(1).

[632] RED delegated act, Article 2(2).

[633] European Commission, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Commission Delegated Regulation Supplementing Directive 2014/53/EU of the European Parliament and of the Council with Regard to the Application of the Essential Requireme' (2021) 23 <https://ec.europa.eu/growth/system/files/2021-10/SWD%282021%29 302_EN_impact_assessment_part1_v3.pdf>.

[634] CSES, "Executive Summary - Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment" (2020), 5.

[635] CSES (n 68), 37.

have to lay down different technical solutions, that is, harmonised standards, which may be used by manufacturers to demonstrate compliance with the essential requirements under scrutiny. Moreover, this will avoid the adoption of non-proportionate solutions. "There are already existing solutions which can be used. For privacy, the "security by design" principle of the GDPR can already be addressed through specific standards. The same applies to the security of payments. For the protection of the network, there is already a pool of best practices and standards that stem from the implementation of the NIS Directive which can be taken as a benchmark and mirrored, where appropriate, into the design of equipment"[636].

Relevant stakeholders highlighted that the cybersecurity standardisation requests of the RED delegated act should be so open, that is, *performance-based* and *technology neutral*, that they will be reusable in future horizontal cybersecurity legislation[637], called for by the new cybersecurity strategy[638], the Council[639], the EDPS[640] and many private actors[641] (as addressed later in section 3.6). Discussions with the ESOs commenced in September 2019[642].

3.4.3 The proposal for a regulation on general product safety: cybersecurity, safety and the IoT

The Proposal for a General Product Safety Regulation, which would repeal Council Directive 87/357/EEC and Directive 2001/95/EC (General Product Safety Directive, GPSD)[643], is yet another case which sheds light on the Commission's approach towards the introduction of cybersecurity requirements in relevant EU product safety legislation. The analysis of the main legal challenges of the GPSD regarding safety and cybersecurity risks posed by cyber-physical systems is not new in

---

[636] European Commission, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Commission Delegated Regulation Supplementing Directive 2014/53/EU of the European Parliament and of the Council with Regard to the Application of the Essential Requireme' (n 613) 52–53.

[637] Dieter Wegener, 'Proposal for a realistic way to implement a "Cybersecurity regulation in Europe"' (2021) ENISA Cybersecurity Standardization Conference, panel 1: Cybersecurity and Radio Equipment Directive – setting up the scene and future work.

[638] European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy (n 15), 9.

[639] Council of the European Union, "Council Conclusions on the cybersecurity of connected devices" (2020), 13629/20, 4-6.

[640] European Data Protection Supervisor, 'Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive' (2021), 8.

[641] BDI, DIN and DKE, 'EU-wide Cybersecurity Requirements - Introduction of horizontal cybersecurity requirements based on the New Legislative Framework and bridge to the EU Cybersecurity Act' (2021) Position paper.

[642] Ben Kokx, 'European Standardization Organisations' (2021) ENISA Cybersecurity Standardization Conference, panel 2: Radio Equipment Directive – setting up the scene and future wo Cybersecurity and Radio Equipment Directive – implementing measures.

[643] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council.

legal scholarly literature[644]. On the other hand, the recent Proposal for a Regulation has not yet received full attention in terms of its impact in cybersecurity regulation.

On 10 December 2021, the EU Parliament Committee on the Internal Market and Consumer Protection published a draft report with significant amendments to the Commission's Proposal. The Rapporteur welcomes the adaptation of the current product safety directive to the risks stemming from connected products, as well as the updated list criteria to evaluate their safety[645]. In the Parliament Draft, Article 7 paragraph 1 – that is, the aspects that shall be taken into account when assessing whether a product is safe – is moved to before Article 6, laying down a new Article 5a. The rationale behind this is that the 'safety assessment' should precede the presumption of safety or, in 'New Legislative Framework' terms, conformity. Thus, "these aspects are valid for all non-harmonised products regardless of whether the presumption of safety is applicable or not"[646]. In this respect, it is worth noting the relevant change apported to the first half sentence of the Article 7(1)/Article 5a: the reference to the non-applicability of Article 5 presumption of safety has been replaced with a much more coherent "when assessing whether a product is safe". As suggested by ANEC and BEUC, those criteria must be binding on economic operators and stakeholders (such as standardisation organisations, national market surveillance authorities, etc.) "for the whole life cycle of a product, from its design to its disposal", without unduly limiting their scope to a post market phase[647].

In this respect, Recital 22 shall be taken into account: "specific cybersecurity risks affecting the safety of consumers as well as protocols and certifications can be dealt with by sectorial legislation. However, it should be ensured, in case of gaps in the sectorial legislation, that the relevant economic operators and national authorities take into consideration risks linked to new technologies, respectively when designing the products and assessing them, in order to ensure that changes introduced in the product do not jeopardise its safety". Thus, when clarifying the aspects that shall be taken into account for assessing the safety of products, that is, the cases where the presumption of safety laid down in Article 5 does not apply, Article 7(1)(h) includes "the appropriate cybersecurity

[644] Fosch-Villaronga and Mahler (n 61) 7–8; Cezary Banasinski and Marcin Rojszczak (n 76), 6–7.

[645] European Parliament, Draft Report on the proposal for a regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council (COM(2021)0346 – C9-0245/2021 – 2021/0170(COD)), 96.

[646] id, 37.

[647] ANEC and BEUC, 'Keeping Consumers Safe from Dangerous Products: How to Make the General Product Safety Regulation a Useful Tool to Ensure Product Safety' (2021) 5 <https://www.beuc.eu/publications/beuc-x-2021-107_general_product_safety_regulation_a_useful_tool_to_ensure_product_safety.pdf>.

features necessary to protect the product against external influences, including malicious third parties, when such an influence might have an impact on the safety of the product"[648].

As regards the link with the 'IoT', AIOTI already expressed its view opposing a Regulation – AIOTI preferred policy option - which would not be technology neutral: "[e]xplicitly mentioning and/or introducing provisions that are technology specific (AI, robotics, IoT) have no added value and would help to push the uptake of innovation due to legal uncertainty"[649]. Whereas 'IoT' is not explicitly mentioned in the legal act, one of the normative novelties introduced by the Proposal is certainly the inclusion into the aspects that shall be taken into account to assess the safety of products of 'connectivity'. In particular, Article 7(1)(b) and 7(1)(c) (in the EU Parliament draft, Article 5a(1)(b) and Article 5a(1)(c)) place the obligation to assess the effect on other products – and the one that other products might have on the product under scrutiny, where it is *reasonably foreseeable* that it will be used with other products, including the interconnection between them. In this respect, a compelling argument raised by DIGITALEUROPE would see as disproportionately wide "by reference to all products that may reasonably foreseeable be used with or connected to the product under assessment". It is recommended thus that these duties shall be limited to the impact assessment of products that are *intended* to be used together or connected[650].

Against the background of including cybersecurity requirements in the legal act, DIGITALEUROPE and Orgalim explicitly opposed the approach proposed by the Commission, albeit from different angles. On the one hand, Orgalim consistently reiterates the necessity to address the issue of cybersecurity for connected products via horizontal harmonised legislation, rather than sectorial legislation, in particular, having regard to EU product safety legal frameworks[651]. On the other hand, DIGITALEUROPE advises the Commission to delete letter (h) of Article 7 to avoid duplicative requirements under different pieces of Union legislation and inconsistencies. As regards the first issue, many cybersecurity requirements for products are also being dealt with under newly proposed instruments related to the Radio Equipment Directive (RED). The second, closely related, leverages

---

[648] Proposal for a Regulation on General Product Safety, Article 7(h).

[649] AIOTI, 'AIOTI response to the public consultation on GPSD', available at <https://aioti.eu/policy-and-strategies/> accessed 8 December 2021.

[650] DIGITALEUROPE, 'DIGITALEUROPE Comments on the Proposed General Product Safety Regulation' (2022) 3 <https://www.digitaleurope.org/resources/digitaleurope-comments-on-the-proposed-general-product-safety-regulation/>.

[651] Orgalim, 'Orgalim Position on the Proposal for a General Product Safety Regulation' (2021) 3 <https://orgalim.eu/position-papers/internal-market-orgalim-position-proposal-general-product-safety-regulation>; Orgalim, 'Proposal for a Horizontal Legislation on Cybersecurity for Networkable Products within the New Legislative Framework' (2020) 4–6 <https://orgalim.eu/sites/default/files/attachment/Proposal for a horizontal legislation on cybersecurity for networkable products within the New Legislative Framework 091120 %28003%29.pdf> accessed 26 January 2022.

the lack of agreed standards on what 'appropriate cybersecurity' entails and upon which economic operators can rely to comply with the legal obligation[652].

Whereas the stance adopted by Orgalim may be theoretically understandable, the approach endorsed by the Commission has clearly taken a different turn as a policy option entailing a horizontal piece of legislation on cybersecurity may realistically not be as timely as one or more delegated acts under the RED[653]. Conversely, the position of DIGITALEUROPE deserves special attention. Thus, the alleged risk of duplication is not well substantiated: the reference to the RED seems to suggest that the cybersecurity requirements of that legal act, coupled with the recently adopted delegated regulation, would comprehensively deal with the challenges posed by connected products. Notwithstanding the wide scope of the RED vis-à-vis connected products, it is ultimately a piece of legislation which covers solely the radio equipment sector. Therefore, some connected products would fall outside the RED's scope, for example, wired connected devices. For this reason, such gaps might be covered by a revised GPSD in its role of 'safety net'[654]. In its function of *lex generalis,* it will fully apply to non-harmonised consumer products and to the harmonised consumer products for the aspects that are not covered by harmonised legislation[655]. In conclusion, rather than insisting on potential overlaps, it is worth looking at how the convergences between the GPSR and RED (and its delegated act) can be exploited.

The second argument presented by DIGITALEUROPE is perhaps more convincing. On the one hand, upon mandate from the Commission, the European Standardisation Organisations (ESOs) shall develop harmonised standards to substantiate cybersecurity (essential) requirements in EU product legislation, providing manufacturers with the possibility (the reliance on harmonised standards being voluntary) of producing the presumption of conformity of products in accordance with harmonised standards. This process will nonetheless require some time. Hence, in the short term, it is reasonable to expect manufacturers to rely on international standards (e.g., ISO/IEC) or in-house developed technical solutions. On the other hand, the lack of agreed standards on what 'appropriate cybersecurity' entails reveals a different piece of the jigsaw, namely the need for a clear, consistent definition of 'cybersecurity', since cybersecurity requirements are currently being included in several

[652] DIGITALEUROPE, 'DIGITALEUROPE Comments on the Proposed General Product Safety Regulation' (n 650) 3.

[653] RED delegated act, 5-6.

[654] European Commission, "Commission Staff Working Document Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council" SWD(2021) 169 final, 10-14.

[655] Ibid, 4.

legislative proposals (i.e., the GPSR, the Machinery Product Regulation and the delegated act under the Radio Equipment Directive – excluding the already in force Medical Device Regulation).

As noted by Orgalim, the requirements vary from one to the other: "in some cases, the product in question must be able to "withstand […] intended and unintended external influences, including malicious attempts from third parties to create a hazardous situation" (Annex III Section 1.2.1 of the Machinery Product Regulation Proposal), in others the cybersecurity features are defined as protection "against external influence" (Proposal for a General Product Safety Regulation, Article 7(1)(h)) or resilience towards "attempts by unauthorised third parties to alter their use or performance" (Proposal for a Regulation on Artificial Intelligence, Article 15(4))[656].

To ensure coherence between the different legal acts, one option could be referring to the essential requirements in terms of cybersecurity provided for in the Medical Device Regulation (MDR)[657], as the MDR marked the beginning of incorporation of cybersecurity aspects within the safety essential requirements into EU product safety legislation. In particular, these requirements would take into account the core principles of information security risk management, therefore including minimum baseline requirements concerning IT security measures, such as protection against unauthorised access. Nevertheless, the level of technical standardisation in terms of cybersecurity in e-Health is more mature than other market sectors, such as consumer devices; as mentioned above, economic operators would find the activity of compliance with the requirements enshrined in relevant legislation to be challenging[658].

Another viable option would be modelling the GPSR cybersecurity requirement on the security objectives laid down in Article 51 of the Cybersecurity Act (see Section 3.3.1), such as protection against unauthorised access or disclosure of information, or protection against accidental or unauthorised lack of availability, verification of access and absence of vulnerabilities, or to follow the security by default principle and to securely update software and hardware[659]. The rationale behind this suggestion being the fact that these cybersecurity objectives are high-level and comprehensive in terms of assets protection coverage in products scenarios. Moreover, the cybersecurity objectives of Article 51 have been compared with the identified requirements of several pieces of EU legislation

[656] Orgalim, 'Orgalim Position on the Proposal for a General Product Safety Regulation' (n 651) 4–5.

[657] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, Annex I, 14.2(d).

[658] See for example the IEC technical standard on medical device software (EN 62304 2006) and ISO medical device risk management (EN 14971 2012) or ISO/IEC 80001 – Application of risk management for IT networks incorporating medical devices.

[659] Regulation (EU) 2019/881, Article 51.

by the project team that has been awarded the contract to carry out a "Study on the need of cybersecurity requirements for ICT products" (as addressed later in section 3.6): the analysis has been based on the Cybersecurity Act as it is one of the most up-to-date and relevant pieces of EU legislation covering cybersecurity for ICT products on a broad spectrum[660].

3.4.4 Cybersecurity requirements in the Medical Devices Regulation

Regulation 2017/745 on medical devices (MDR)[661] establishes a regulatory framework for the production, the placing on the market and putting into service of medical devices and their accessories on the EU market[662]. A medical device is whatever instrument, software or article *intended by the manufacturer* to be used, alone or in combination, for human beings for specific medical purposes (e.g., diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, injury, disability, etc.)[663]. In this respect, in *Snitem and Philips France*, the CJEU clarified that software, of which at least one of the functions makes it possible to use patient-specific data for medical purposes (such as detecting contraindications, drug interactions and excessive doses) is, in respect of that function, a medical device, even if such software does not act directly in or on the human body[664]. As a result, the Court seems to adopt a risk-based and case-by-case approach – coming close to the U.S. FDA system[665] - in order to qualify the software or device at stake as medical device: the *actual* function of the asset becomes as important as the intended use declared by the manufacturer[666].

The harmonised Regulation mandates that, in order to be placed on the market and put into service in the Single Market, medical devices must meet the safety requirements set out in Annex I of the MDR[667]. In accordance with the principles of the NLF, manufacturers must undertake a conformity assessment before placing the product on the market[668], involving clinical safety evaluations[669]. Following a risk-based approach, manufacturers shall establish, document, implement and maintain

---

[660] Wavestone - CEPS - CARSA - ICF (n 539) 53.

[661] n 334.

[662] Regulation (EU) 2017/745, recital 2.

[663] id, Article 2(1), recital 19: "[w]hile software for general purposes, even when used in a healthcare setting, or software intended for life-style and well-being purposes is not a medical device".

[664] Case C-329/16 *Snitem and Philips France* [2018] ECLI:EU:C:2017:947.

[665] Paul Quinn, 'The EU Commission's Risky Choice for a Non-Risk Based Strategy on Assessment of Medical Devices' (2017) 33 Computer Law & Security Review 361, 369–370.

[666] Aiste Gerybaite, 'Exploring the Regulatory Interplay in Health Internet of Everything: Digital Health Technologies, Data Protection and Cybersecurity' [2022] Forthcoming 1, 8.

[667] Regulation (EU) 2017/745, Article 5(2).

[668] ibid, Article 52.

[669] ibid, Article 61.

a system for risk management (detailed in Annex I)[670] and a post-market surveillance system in a manner that is proportionate to the risk class and appropriate for the type of device[671]. Indeed, medical devices must be divided in certain classes according to the intended purpose of the devices and their inherent risks[672]. In other words, the classification of the device, as per Annex VIII MDR, "dictates the appropriate conformity assessment procedure: the higher the classification, the greater the level of assessment required by the notified bodies"[673].

As mentioned in the previous section, the MDR is the first legal act within EU product safety legislation to incorporate cybersecurity requirements. Annex I of the Regulation, which sets out general safety and performance requirements, obliges manufacturers of medical devices to fulfil minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access. Thus, devices shall be designed and manufactured to address and minimise "the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts"[674]. Most of the provisions are indeed dedicated to software. In particular, software should be developed and manufactured "in accordance with the state of the art taking into account the principles of development life cycle[675], risk management, including information security, verification"[676] and the specific features of the mobile computing platform in combination with which it is used[677]. The last requirement relevant to cybersecurity addresses "minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended"[678].

---

[670] ibid, Article 10(2).

[671] ibid, Article 83.

[672] ibid, Article 51(1).

[673] Magali Contardi, 'Changes in the Medical Device's Regulatory Framework and Its Impact on the Medical Device's Industry: From the Medical Device Directives to the Medical Device Regulations' (2019) 12 Erasmus Law Review 166, 170.

[674] MDR, Annex I, 14.2(d).

[675] ENISA, 'Good Practices for Security of IoT Secure Software Development Lifecycle' (2019).

[676] MDR, Annex I, 17.2

[677] MDR, Annex I, 17.3.

[678] MDR, Annex I, 17.4.

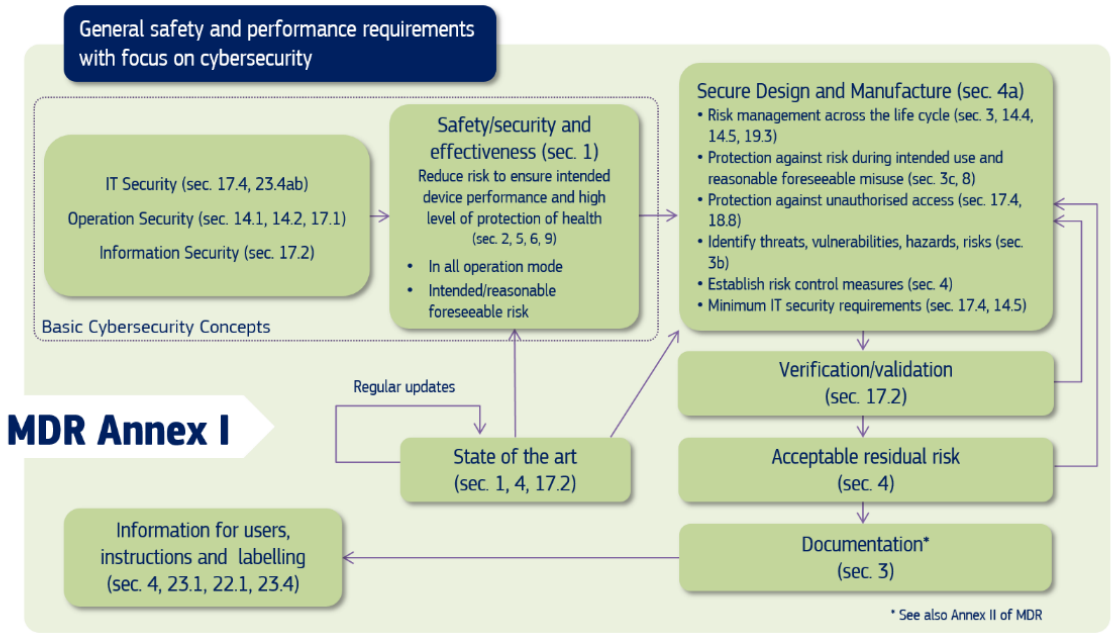


Figure 6: MDR Annex I cybersecurity requirements[679]

In the context of the IoT, if the device is intended for use in combination with other devices or equipment the whole combination – including the connection system – shall be safe and shall not impair the specified performance of the devices[680]. In this scenario, the classification rules of the medical device and another (non-medical) device with which the former is intended to be used in combination shall apply separately to each of the devices, as "[a]ccessories are classified in their own right separately from the device with which they are used"[681]. To make things more complex, Article 1(3) MDR states that devices with both a medical and a non-medical intended purpose shall cumulatively fulfil the legal requirements applicable to devices with an intended medical purpose and those applicable to devices without an intended medical purpose.

Therefore, it may be the case that within an IoT ecosystem different requirements, in terms of cybersecurity, stemming from different legal frameworks (e.g., MDR and Machinery Directive[682]), apply (i) to different devices that may be manufactured by the same actor or (ii) cumulatively to the same device. Two different legal challenges arise, in particular, in regard to the latter scenario, potentially leading to legal uncertainty.

---

[679] Medical Device Coordination Group, 'Guidance on Cybersecurity in Medical Devices' (2019) 5 <https://ec.europa.eu/docsroom/documents/41863>.

[680] MDR, Annex I, 14.1.

[681] *Snitem and Philips France* (n 663), §10.

[682] Fosch-Villaronga and Mahler (n 323) 8.

The first aspect under scrutiny investigates how to exploit the potential synergies (or mechanisms of legal coordination and cooperation[683]) between cybersecurity requirements under different EU legal acts in the health sector. In this respect, the MDR addresses only manufacturers, while leaving other actors involved in the use of a medical devices, such as hospitals and other care providersm, off the hook[684]. As seen in Section 3.2, these actors would nonetheless face cybersecurity responsibilities and duties under the NIS Directive, as OES; as such, they are required to manage the cybersecurity risks posed to the network and information systems – such as medical devices – which they use in their operations (Article 14(1) NIS). In other words, "obligations towards establishing information security of a specific integrated device effectively remain with the Health Delivery Organisation if it has mandated the integrator to connect a given medical device to the clinical/hospital IT network"[685].

As regards the issue of overlapping duties that would create legal uncertainty, if the cybersecurity requirements of the different legal acts that would cumulatively apply significantly diverge from one another – as seen in the previous section when discussing divergences in the content of cybersecurity requirements in product legislation, the standard of protection may differ. Thus, the set of cybersecurity requirements of the MDR is more granular, scalable and detailed (including the security by design principle, security risk management, security capabilities or controls, risk assessment, minimum requirements, validation/verification and life-cycle considerations) when compared to the framework of the RED or the Proposal for a Machinery Regulation (next section). In terms of cybersecurity compliance, it can be concluded that once the manufacturer fulfils the obligations laid down in the MDR, it should not incur liability under the cybersecurity obligations of other legal regimes, to the extent permitted by existing EU or national law.

Lastly, in order to comply with high-level requirements, rather than introducing (new) mandatory technical security requirements[686], manufacturers can use harmonised technical standards, published in the EU Official Journal, to provide a presumption of conformity with relevant legislation. On 26 June 2020, CEN and CENELEC rejected the Commission's implementing decision M/565 requiring European Standardisation Organisations to standardise a series of existing regulations and new regulations to be drawn up as regards medical devices, in support of the Medical Devices Regulation MDR (EU) 2017/745 and the In Vitro Diagnostic Medical Devices Regulation IVDR (EU)

---

[683] Gerybaite (n 666) 10–12.

[684] Fosch-Villaronga and Mahler (n 323) 7.

[685] Medical Device Coordination Group (n 679) 12.

[686] Anton Reindl and others, 'Legal and Technical Considerations on Unified, Safe and Data-Protected Haptic Telepresence in Healthcare' [2021] Proceedings of the 2021 IEEE International Conference on Intelligence and Safety for Robotics 239, 242.

2017/746[687]. Eventually, on 14 April 2021, the Commission filed a new standardisation request to ESOs whereby it requested a revision of existing harmonised standards in support of the MDR, including, in particular, EN ISO 14971:2019 on application of risk management to medical devices; EN 62304:2006+A1:2015 on (medical devices) software lifecycle processes; EN IEC 82304-1 Health Software Part 1: General requirements for Product Safety; EN ISO/IEC 80001-1 Application of Risk Management for IT Networks Incorporating Medical Devices[688]; EN 62366-1:2015+AC:2015+AC:2016+A1:2020 Medical devices - Application of usability engineering to medical devices. At the same time, the Commission also requested new harmonised standards to be drafted, the most relevant to cybersecurity being IEC/TR 60601-4-5 Medical Electrical Equipment – Part 4-5. Safety related technical security specifications for medical devices[689]. CEN and Cenelec will provide the Commission with the joint final report by 30 June 2024[690].

3.4.5 The proposal for a machinery regulation and IoT cybersecurity

Albeit the current Machinery Directive[691] is outside the NLF, the Proposal for a Regulation on Machinery Products[692], repealing the Directive, would lay down cybersecurity requirements for the design and construction of machinery products while seeking "to enhance the enforcement of the legal act through the alignment to the NLF"[693]. Thus, the impact assessment accompanying the Proposal highlights that most stakeholders largely supported the alignment of the Machinery

---

[687] European Commission, 'COMMISSION IMPLEMENTING DECISION M/565 of 15.5.2020 on a standardisation request to the European Committee for Standardization and the European Committee for Electrotechnical Standardization as regards medical devices in support of Regulation (EU) 2017/745 of the European Parliament and of the Council and in vitro diagnostic medical devices in support of Regulation (EU) 2017/746 of the European Parliament and of the Council' (2020).

[688] For further analysis, see Scott Anderson and Trish Williams, 'Cybersecurity and Medical Devices: Are the ISO/IEC 80001-2-2 Technical Controls up to the Challenge?' (2018) 56 Computer Standards & Interfaces 134.

[689] European Commission, 'COMMISSION IMPLEMENTING DECISION of 14.4.2021 on a standardisation request to the European Committee for Standardization and the European Committee for Electrotechnical Standardization as regards medical devices in support of Regulation (EU) 2017/745 of the European Parliament and of the Council and in vitro diagnostic medical devices in support of Regulation (EU) 2017/746 of the European Parliament and of the Council' (2021), Article 1(1).

[690] ibid Article 3(3).

[691] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery.

[692] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on machinery products" COM(2021) 202 final.

[693] Irmgard Anglmayer, 'Briefing Implementation Appraisal EPRS, Machinery Directive: Revision of Directive 2006/42/EC' (2021) 11 <https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2021)694206> accessed 18 October 2021.

Directive to the NLF, addressing *inter alia* shortcomings in the area of market surveillance – generally seen as insufficient and ineffective[694], and conversion into a regulation[695].

The directive applies to all new machinery placed on the market for the first time, regardless of its origin i.e., whether manufactured within or outside the EU. The Parliamentary implementation appraisal of September 2021 claimed that the Directive's "scope of application is very broad, encompassing a vast array of machinery for industrial and private use, including construction machinery, lawnmowers, powered hand-tools, as well as certain modern machinery, including 3D printers, e-bikes, robots and drones"[696].

Nevertheless, with specific regard to modern machinery, the scope of the proposed Regulation would differ significantly. For instance, whereas the e-bikes – and light vehicles more generally (such as electrically power-assisted cycles, hover boards, or self-balancing scooters) – fall under the scope of the Directive[697], they are excluded from the Commission's Proposal. Thus, following the suggestions made in the impact assessment[698], Art 2(2)(e) explicitly excludes "vehicles which have as their only objective the transport of goods or persons by road, air, water or rail except for machinery mounted on those vehicles" from the Regulation's scope. Instead, with regard to drones, the relevant applicable law is the Commission Delegated Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. Article 4(2) of that legal act states that "UAS (i.e., drones) that are not toys within the meaning of Directive 2009/48/EC shall comply with the relevant health and safety requirements set out in Directive 2006/42/EC only in relation to risks other than those linked to the safety of the UA flight". Therefore, the relevant essential requirements set out in Directive 2006/42/EC shall apply to drones only insofar as they refer to aspects not related to the flight.

Moreover, the Regulation would not apply to many electrical and electronic (possibly connected) products, insofar as they fall within the scope of application of Directive 2014/35/EU or Directive

---

[694] ibid 4.

[695] European Commission, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the Proposal for a Regulation of the European Parliament and of the Council on machinery products' SWD(2021) 82 final, 48.

[696] Anglmayer (n 693) 2.

[697] Parliamentary question E-003051-19 to the Commission by Seán Kelly (PPE) (1 October 2019), <https://www.europarl.europa.eu/doceo/document/E-9-2019-003051_EN.html> accessed 4 February 2022. Ms Bieńkowska on behalf of the European Commission answered that "electric bicycles are already covered by the machinery Directive 2006/42/EC" <https://www.europarl.europa.eu/doceo/document/E-9-2019-003051-ASW_EN.html> accessed 4 February 2022.

[698] European Commission, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the Proposal for a Regulation of the European Parliament and of the Council on machinery products' (n 372), 44.

2014/53/EU: household appliances intended for domestic use; audio/video equipment, information technology equipment; office machinery; low-voltage switchgear and control gear; electric motors[699]. All in all, the proposed Regulation would not cover a wide range of IoT devices.

The evaluation assessment also pointed out a number of regulatory gaps that should be addressed in the Directive revision. In particular, the assessment identified six problems: i) insufficient coverage of new risks relating to emerging digital technologies; ii) legal uncertainty due to a lack of clarity on the scope and definitions and possible safety gaps in traditional technologies; iii) insufficient provisions for high-risk machines; iv) monetary and environmental costs; v) inconsistencies with other pieces of EU product-safety legislation; vi) divergences in interpretation due to transposition[700]. This section will critically elaborate on the first problem, as the revision process is based on the assumption that the Directive is not adequate as such, despite its technology-neutral design, to cope with the challenges arising from progress in digital technologies, in particular, having regard to cybersecurity concerns[701].

Against this background, the aim of the Commission is to address those cybersecurity risks having an impact on safety, such as preserving machinery against malicious third party attacks, without precluding the application of other Union legislation specifically addressing cybersecurity aspects to machinery products [702]. In this respect, Annex III to the Proposal lays down the essential health and safety requirements relating to the design and construction of machinery products. Importantly, as regards the presumption of conformity of machinery products with the essential health and safety requirements set out in the Proposal, besides the NLF reference to harmonised standards, the co-legislator foresee the possibility for manufacturers to refer to certificate or statement of conformity issued under a relevant cybersecurity scheme adopted pursuant to and in accordance with Article 54(3) of Regulation (EU) 2019/881[703].

In view of addressing the 'cybersecurity risk' with an impact on safety, the Proposal seemingly restricts – in Recitals 22 and 43 – the scope of the new requirements to malicious third-party actions, thereby unduly moving away from more high-level and all-encompassing understandings of cybersecurity risks, enshrined for example in the Cybersecurity Act. Nevertheless, a closer look at the requirements under scrutiny, namely 1.1.9 and 1.2.1, reveals a more 'agnostic' perspective in

---

[699] Proposal for a Regulation on Machinery Products, Article 2(2)(m).

[700] Mari Tuominen and Solène Festor, 'Initial Appraisal of a European Commission Impact Assessment: Revising the Machinery Directive', vol PE 694.208 (2021) 1–2 <http://www.europarl.europa.eu/RegData/etudes/note/join/2013/507504/IPOL-JOIN_NT(2013)507504_EN.pdf>.

[701] Proposal for a Machinery Regulation, Recital 11.

[702] ibid Recital 22.

[703] ibid Article 17(5); Recital 43.

terms of the sources of security threats. Thus, the requirement 1.1.9 explicitly addresses protection against *accidental* and intentional corruption. Moreover, the incipit of the article is rather broad: "the machinery product shall be designed and constructed so that the connection to it of another device, via any feature of the connected device itself or via any remote device that communicates with the machinery product *does not lead to a hazardous situation* [emphasis added]". Moreover, accidental corruption is also taken into account in ensuring adequate protection to software and data that are critical for the machinery product's compliance with the relevant health and safety requirements[704]. On the other hand, requirement 1.2.1 mandates that, following a risk-based approach, control systems shall withstand "the intended operating stresses and intended and *unintended* external influences, including malicious attempts from third parties to create a hazardous situation [emphasis added]". In conclusion, the reference to "malicious third-party attempts" made in the legal act shall be carefully assessed against the actual content of the essential requirements of Annex III which broaden the scope of protection to accidental corruption, unintended external influence and hardware fault (ESHR 1.2.1(b)).

Against this background, as noted by CEN – CENELEC, one of the cornerstone principles of the New Legislative Framework is that harmonised legislation specifies essential requirements within the boundaries of a product's 'intended use' and 'reasonably foreseeable misuse'. "The 2016 edition of the Blue Guide clearly states in Section 2.7 that this consideration shall result from "lawful and readily predictable human behaviour". Hence intentional unlawful human behaviour should thus not fall under the "intended use" or "reasonably foreseeable misuse" under any NLF-legal acts, such as the proposed regulation. […] Every kind of intentional violation (sabotage/spying) of a machine is de facto a criminal act" [705]. As a result, according to the European standardisation organisations, the new EHSR 1.1.9 and 1.2.1(a) are arguably in contradiction with the above-mentioned basic principle of the NLF as stated in the Blue Guide; hence, they should be deleted.

Albeit from a different perspective, DIGITALEUROPE also criticises the reference to 'third parties' malicious attempts' of the proposal on the grounds that they would not be possible to foresee. "DIGITALEUROPE recommends that the Regulation only applies to those risks that are known when the equipment is placed on the market or put into service. State-of-the-art cyber security standards

[704] ibid Annex III, 1.1.9.

[705] CEN - CENELEC, 'CEN-CENELEC Response to the European Commission' s Public Consultation on the Draft Machinery Regulation' (2021) 5–6 <https://www.cencenelec.eu/media/Policy Opinions/2021-07-07_cen-cenelecpositionondraftmachineryregulation.pdf> accessed 4 February 2022.

can be applied at the time the equipment is placed on the market or put into service, but not beyond that point"[706].

3.4.6 The right answer?

Section 3.4 showed the Commission's approach to the ever-growing number of unsecure IoT devices in the Single Market, consisting of a revision of product safety legislation to include cybersecurity essential requirements. As mentioned above, safety legislation is primarily focused on the design and manufacturing phases, as linked to the placing and making available of products on the market, whereas cybersecurity – and IoT specifically – requires dynamic risk management, that must be ensured throughout the whole life cycle of the devices[707].

Thus, the inclusion of cybersecurity requirements in sectoral legislation, such as the Machinery Regulation or other product safety legal acts, is not considered appropriate by many stakeholders, with EUROSMART being an exception[708]. DIGITALEUROPE[709], Orgalim[710], CEN – CENELEC[711], Bundesverband der Deutschen Industrie (BDI)[712] and the European Economic and Social Committee (EESC)[713] argue that the Commission has embarked upon a path towards fragmented and contradictory legal requirements. Albeit a sectorial approach vis-à-vis the issue of connected products security may prove to be effective in the short term, only a horizontal legislation will address the problem at the core in the most efficient way[714]. The last section of this Chapter (3.6) will elaborate on this policy option.

Against this backdrop, the next section sheds light on how broader cybersecurity administrative, procedural and organisational requirements introduced by the revised NIS Directive (NIS2) may

---

[706] DIGITALEUROPE, 'DIGITALEUROPE Position Paper on the New Machinery Regulation' (2021) 4.

[707] Charlotte Ducuing, 'Towards an Obligation to Secure Connected and Automated Vehicles "by Design"?', *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia 2019) 203.

[708] EUROSMART, 'Revision of the Machinery Directive: Answer to the European Commission Public Consultation' (2019) <https://www.eurosmart.com/revision-of-the-machinery-directive/> accessed 4 February 2022.

[709] DIGITALEUROPE, 'DIGITALEUROPE Position Paper on the New Machinery Regulation' (n 706) 7–8.

[710] Orgalim, 'Proposal for a Horizontal Legislation on Cybersecurity for Networkable Products within the New Legislative Framework' (n 651).

[711] CEN - CENELEC (n 705) 6.

[712] BDI, 'EU-Wide Cybersecurity Requirements: Introduction of Horizontal Cybersecurity Requirements Based on the New Legislative Framework and Bridge to the EU Cybersecurity Act' (2021) <https://www.din.de/resource/blob/788018/f9708b36c89b2e527bcb1a66f523827a/2021-bdi-din-dke-position-cybersicherheit-europa-en-final-data.pdf> accessed 6 June 2022.

[713] European Economic and Social Committee, 'Revision of the Machinery Directive ' (2021) <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/information-reports/revision-machinery-directive> accessed 6 June 2022.

[714] Wavestone - CEPS - CARSA - ICF (n 539) 256–257; Pier Giorgio Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' (2022) 36 International Review of Law, Computers & Technology 118.

contribute to strengthening IoT cybersecurity when coupled with product-related requirements laid down in EU product legislation[715].

3.5 The Revision of the NIS Directive: the NIS2 and the IoT

On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented the new European Cybersecurity Strategy[716], a key component of the European Digital Transition Plan[717], the Recovery Plan[718] and the European Security Strategy of July 2020[719]. The strategy defines three areas of EU action, for increased protection of citizens, businesses and institutions, through the deployment of regulatory, investment and policy instruments. These are: (1) resilience, technological sovereignty and leadership, (2) developing operational capabilities for prevention, deterrence and response, and (3) promoting a global and open cyberspace.

The Commission aimed at further improving the prevention, resilience and incident response capabilities of public and private entities, competent authorities, and the Union as a whole, in the field of cybersecurity. This ambitious objective led to two legislative proposals: the revision of the NIS Directive and a new Directive on Critical Entity Resilience[720]. On 27 December 2022, Directive (EU) 2022/2555 (hereinafter, NIS2) was published in the Official Journal of the EU and entered into force on 16 January 2023[721]. The fast-paced action of the Commission in this sector underlines the increasing centrality of cybersecurity issues in the Union's political agenda.

The NIS2 seeks to modernise the existing legal framework and addresses several weaknesses that prevented the existing Directive from unlocking its full potential. The explanatory memorandum of the Proposal for the NIS 2 acknowledged that the NIS Directive had contributed to improving cybersecurity capabilities at national level by requiring Member States to adopt national cybersecurity strategies and to appoint cybersecurity authorities. The NIS also had increased cooperation between

---

[715] DIGITALEUROPE, 'Setting the Standard: How to Secure the Internet of Things' (n 559) 9.

[716] European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy (n 619).

[717] European Commission, 'Shaping Europe's Digital Future ' <https://digital-strategy.ec.europa.eu/it> accessed 14 June 2022.

[718] European Commission, 'Recovery Plan for Europe ' (2020) <https://ec.europa.eu/info/strategy/recovery-plan-europe_en> accessed 14 June 2022.

[719] European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy' (n 214).

[720] European Commission, *Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities* COM(2020) 829 final.

[721] On 27 December 2022, Directive (EU) 2022/2557 and Regulation (EU) 2022/2554, namely the directive on the resilience of critical entities and DORA regulation respectively, have also been published on the EU OJ.

Member States at Union level by setting up various fora facilitating the exchange of strategic and operational information. A further success had been the improvement of the cyber resilience of public and private entities in seven specific sectors (energy, transport, banking, financial market infrastructures, healthcare, drinking water supply and distribution, and digital infrastructures) and across the three digital services providers (online marketplaces, online search engines and cloud computing services) by requiring Member States to ensure that operators of essential services and digital service providers put in place cybersecurity requirements and report incidents[722].

Nevertheless, the evaluation of the functioning of the NIS Directive highlighted six major areas of concern. First, the overly limited scope in terms of the sectors covered (due to the higher degree of IoT interconnectedness and the exclusion of sectors providing key services to the society). Second, the lack of clarity as regards the scope of OES and the national competence over DSP, resulting in fragmentation as certain types of entities have not been identified in all Member States. Third, the significant fragmentation among Member States when laying down security and incident reporting requirements for OESs, creating additional burden for companies operating in more than one Member State. Fourth, the ineffective supervision and enforcement regime, as Member States have been very reluctant to apply penalties. Fifth, the different level of progress among Member States in dealing with cybersecurity risks. Finally, the lack of information sharing between Member States[723].

Therefore, the NIS2 has been structured around several interrelated policy areas with a view to addressing the above-mentioned regulatory failures. In particular, they regard: i) subject matter and scope; ii) national cybersecurity frameworks; iii) cooperation; iv) cybersecurity risk management and reporting obligations; v) jurisdiction and registration; vi) information sharing; vii) supervision and enforcement[724].

Among the systemic and structural changes envisaged by the NIS2[725], this section aims to test whether and to what extent the NIS2 would ensure a higher standard of protection against unsecure IoT devices

---

[722] European Commission, 'Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148 COM(2020) 823 Final' (2020) <https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF> accessed 28 October 2021.

[723] ibid 6.

[724] ibid 9–11.

[725] Sandra Schmitz-Berndt, 'Cybersecurity Is Gaining Momentum - NIS 2.0 Is on Its Way' (2021) 7 European Data Protection Law 580 <https://www.fnr.lu/projects/> accessed 23 February 2022; Raffaella Brighi and Pier Giorgio Chiara, 'La Cybersecurity Come Bene Pubblico: Alcune Riflessioni Normative a Partire Dai Recenti Sviluppi Nel Diritto Dell'Unione Europea' (2021) 21 Federalismi.it 18; Thomas Sievers, 'Proposal for a NIS Directive 2.0: Companies Covered by the Extended Scope of Application and Their Obligations' (2021) 2 International Cybersecurity Law Review 223; Elisabetta Biasin and Erik Kamenjašević, 'Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals' (2022) 3 International Cybersecurity Law Review 163.

by taking into account and addressing the following issues: i) the enlarged scope of the NIS2, in particular, taking into account the 'manufacturing' sector; ii) the vulnerability disclosure and handling procedures; and, iii) new cybersecurity requirements for the supply chain. The analysis that follows primarily builds on a previous publication by the same author of this thesis[726].

3.5.1 The enlarged scope of the NIS2

The explanatory memorandum to the NIS2 highlights that the "increased digitisation in recent years and a higher degree of interconnectedness" are crucial factors which contributed to the gradual inadequacy of the too limited scope of the NIS Directive, which "no longer reflects all digitised sectors providing key services to the Union"[727]. The IoT, implicitly evoked by the keyword 'interconnectedness', is in this regard one of the technological developments that prompted the EC to act.

Against this background, the NIS2 applies to public and private 'essential entities' (EEs) and 'important entities' (IEs)[728], replacing the NISD distinction between operators of essential services and digital services providers. In this respect, the broadening of the scope hinges on the level of criticality of the sector or of the type of service provided by the entity. The EEs – which are considered to operate in more critical sectors – are listed in Annex I NIS2 (on top of the sectors among which the OES were identified under the NISD, namely energy; transport; banking; financial market infrastructures; health; drinking water; digital infrastructure). Accordingly, the new sectors in scope are: wastewater; public administration[729] and space. Annex II NIS2 lists the sectors where the IEs are to be found and include the previously non-encompassed sectors postal and courier services; waste management; manufacture, production and distribution of chemicals; food production, processing and distribution; manufacturing and digital providers.

To overcome the wide divergences among Member States in terms of identification of the OESs falling into the scope of the NIS legal framework, Art. 2(1) NIS2 lays down a 'size-cap rule' criterion which exclude small and micro enterprises. However, as acknowledged by Recital 7, "Member States should also provide for certain small enterprises and microenterprises, as defined in Article 2(2) and (3) of that Annex, which fulfil specific criteria that indicate a key role for society, the economy or for

[726] Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' (n 714).

[727] European Commission, 'Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148 COM(2020) 823 Final' (n 722) 6.

[728] Art. 2(1) NIS2.

[729] The Council, in the trialogue discussions proposed to exclude public administrations.

particular sectors or types of service to fall within the scope of this Directive"[730]**.** Accordingly, Art. 2(2) states that, regardless of their size, this Directive also applies to essential and important entities if the entity fulfils certain requirements[731]. Notably, Art. 7(2)(i) NIS2 mandates Member States to adopt, as part of the national cybersecurity strategy, policies with a view of "strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs".

The rationale underlying the paradigm shift in terms of the scope of application of the Directive is to provide comprehensive coverage of the sectors that are of vital importance to key societal and economic activities[732] and, as such, deserved to be praised. However, as highlighted by several stakeholders, the absence of granular and scalable requirements based on actual risk (e.g., business-to-business versus business-to-consumer models) may turn the NIS2 into "blanket legislation covering most ICT services without any real distinctions"[733].

With regard to the IoT, it is worth mentioning that Annex II lists as IEs those entities operating in the manufacturing sector. The six sub-sectors of the 'manufacturing' sector (medical, computer, electronic, electrical, machinery, motor vehicles and transport equipment) are undoubtedly relevant to the IoT market. Annex II of the NIS2 makes reference to the 'NACE Rev. 2 classification of economic activities' to further substantiate which types of undertakings fall within the sub-sectors under scrutiny[734].

Recalling the outcomes of section 3.2.3, connected devices forming part of the network and information systems of EEs and IEs would still be covered by the scope *rationae personae* of the NIS2. However, the NIS2 would not *directly* tackle the problem of unsecure IoT products and related services as the Directive would not impose product-related requirements on manufacturers and developers, even though they now fall within the scope of the NIS2 as IEs. Thus, sectoral product safety legislation already mandates cybersecurity product technical requirements[735]. However, even

---

[730] Recital 9 NIS2.

[731] For example, the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities (Art. 2(2)(b) NIS2).

[732] Recital 6 NIS2.

[733] DIGITALEUROPE, 'DIGITALEUROPE Position on the NIS2 Directive' (2021) 4; BDI, 'Position Paper on NIS 2-Directive' (2021) 7.

[734] For example, the manufacturing of computers and electronic products include inter alia consumer electronics, electronics components and communication equipment (NACE Rev. 2 – Statistical classification of economic activites in the European Community, division 26, 69).

[735] DIGITALEUROPE, 'DIGITALEUROPE Position on the NIS2 Directive' (n 733) 6.

if the NIS2 maintains a principle-based character, laying down procedural and 'organisational'[736] requirements, two regulatory novelties introduced by the revision of the NISD may overlap with product-related requirements. In particular, this would be the case vis-à-vis: i) the disclosure and handling procedures for vulnerabilities; ii) cybersecurity requirements in terms of secure supply chain relationships.

3.5.2 A procedural framework for vulnerability disclosure

As seen in Chapter 2, the exchange of information on vulnerabilities is one main area of intersection between the public and private sector, as testified by the growing number of public-private partnership (PPPs) initiatives to strengthen cybersecurity.

In this respect, Article 12 NIS2 lays down a procedural framework for coordinated vulnerability disclosure. Each Member State has to designate a CSIRT as the coordinator of this process. The CSIRT will act as a trusted intermediary, where required facilitating the interaction between the reporting entity and the ICT service or product manufacturer or provider[737]. It is up to ENISA, instead, to develop and update a "European Vulnerability Register". The database shall contain information describing the vulnerability, the ICT products or services concerned, the severity of the vulnerability if exploited, the availability of relevant patches and, if not available, guidance to users of vulnerable products and services on how to mitigate the risks[738]. It is clear, therefore, how the intention of the Commission is to increasingly encourage an approach of close cooperation between private and public actors in the cybersecurity field.

Importantly, the original text proposed by the Commission has been amended by the Parliament in the sense of specifying that only those vulnerabilities for which a patch is available shall be listed in the vulnerability database[739]. Otherwise, this provision – which certainly does go in the direction of greater security – could create a paradoxical situation, where a vulnerability was published without any mitigation measures, thus facilitating the work of attackers.

Albeit only in the recitals, the NIS2 affirms that "entities that develop or administer network and information systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and disclosed by third parties, the

---

[736] DIGITALEUROPE, 'Setting the Standard: How to Secure the Internet of Things' (2021) 9.

[737] Art. 12(1) NIS2.

[738] Art. 12(2) NIS2.

[739] European Parliament, REPORT on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)), Amendment 127 Proposal for a directive Article 6 – paragraph 2.

manufacturer or provider of ICT products or ICT services should also put in place the necessary procedures to receive vulnerability information from third parties"[740]. Thus, Art. 21(2)(e) stipulates that entities shall take into account – as a baseline cybersecurity management measure (addressed in the next section) – the "security in network and information systems acquisition, development and maintenance, *including vulnerability handling and disclosure* [emphasis added]".

The Directive does not contain an 'obligation to patch' for manufacturers within a specific timeframe[741], similar to what Directive (EU) 2019/771 has implemented with respect to sellers (but not manufacturers!)[742], as it would not be the proper legal instrument for implementing such an obligation, for the reasons discussed in the above section. Rather, this might be better achieved by the incoming Cyber Resilience Act (addressed in section 3.6).

If it is true that giving manufacturers more leeway in terms of vulnerability handling would come at a cost for consumers in terms of security, that has been welcomed by industry, as companies, when developing patches, "should not encounter additional outside pressure which could lead to a deterioration of the quality of the work"[743].

3.5.3 Cybersecurity management measures

Another legal challenge in terms of overlap with cybersecurity 'product requirements' is the cybersecurity management measure focusing on supply chain relationships. While adhering to a risk-based approach already envisioned by the NIS Directive[744], the NIS2 introduces an appreciable element of novelty, that is, a list of minimum cybersecurity measures to be taken indiscriminately by EEs and IEs to manage the risks posed to their NIS. These measures are:

(a) policies on risk analysis and information system security;

---

[740] Recital 58 NIS2.

[741] European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy (n 619) 9.

[742] See Art. 7(3) Directive (EU) 2019/771 (Sale of Goods Directive). Cfr. *inter alia* with: André Janssen, 'The Update Obligation for Smart Products – Time Period for the Update Obligation and Failure to Install the Update' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Smart Products: Münster Colloquia on EU Law and the Digital Economy VI* (Nomos Verlag 2022); Christiane Wendehorst, 'The Update Obligation – How to Make It Work in the Relationship between Seller, Producer, Digital Content or Service Provider and Consumer' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Smart Products: Münster Colloquia on EU Law and the Digital Economy VI* (Nomos Verlag 2022). See also Roman Dickmann, 'Vulnerability Management as Compliance Requirement in Product Security Regulation — a Game Changer for Producers ' Liability and Consequential Improvement of the Level of Security in the Internet of Things?' [2022] International Cybersecurity Law Review 4–5.

[743] BDI, Position on ITRE-Amendments to NIS 2-Directive German industry's position on the ITRE Committee's amendments to the Commission proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 6.

[744] Art. 21(1) NIS2: "Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services".

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate [745].

In particular, for the purpose of this work, emphasis will be placed on the requirement to address the cybersecurity of the ICT supply chain, including security-related aspects concerning the relationships between each entity and its suppliers. The rationale underlying these high-level technical measures[746] must be found in an attempt to prevent incidents, where malicious actors compromise the security of an entity's NIS by exploiting vulnerabilities affecting third party products and services[747]. As reiterated in the previous Chapters, the majority of IoT devices is comprised by a multitude of components from different hardware and software vendors, part of which could even be accounted for by small companies, including start-ups[748]. As a consequence, the attack surface is expanded globally[749].

Importantly, when implementing risk management measures referred to Art. 21(2)(d), EEs and IEs "shall take into account the vulnerabilities specific to each supplier and service provider and the

---

[745] Art. 21(2) NIS2.

[746] Interestingly, the Commission will adopt implementing acts (Art. 21(5) NIS2) to lay down the technical and the methodological specifications of the elements referred to in paragraph 2 of Art. 21 and to take account of new cyber threats, technological developments or sectorial specificities.

[747] Recital 43 NIS2.

[748] See <https://www.startus-insights.com/innovators-guide/5-top-internet-of-things-startups-impacting-logistics-supply-chain/> accessed 21 October 2021; European Commission, "An SME Strategy for a sustainable and digital Europe" COM(2020) 103 final, 1.

[749] AIOTI, 'AIOTI Feedback to the Public Consultation on the Revised Draft NIS Directive (NIS2)' (2021), 3.

overall *quality of products* and cybersecurity practices of their suppliers and service providers [emphasis added]"[750]. To assist entities in appropriately managing the cybersecurity risks related to supply chain, Article 22 NIS2 introduces coordinated supply chain risk assessments – which will take into account also non-technical risk factors (e.g., geopolitical) – mirroring Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[751].

Notwithstanding this, NIS2 supply chain provisions may prove to be burdensome for EEs and IEs as it is unclear how entities shall ensure that suppliers comply with relevant legal requirements[752]. Furthermore, a combined reading of Art. 21(2)(d) and 21(3) would *indirectly* address products security because, by requiring consideration of the cybersecurity of suppliers' systems, "manufacturers will have strong incentives to enhance the security controls in their products"[753].

Lastly, to demonstrate compliance with certain requirements of Art. 21, the Commission foresees the possibility for Member States to require mandatory certification for ICT products, services and processes under specific ECCS adopted pursuant to Art. 49 CSA[754]. Importantly, the Commission is empowered to adopt delegated acts (DA), specifying which categories of NIS entities shall be required to use certified ICT products, services and processes, or obtain a certificate and under which scheme[755]. Contrary to the previous version of Art. 24(2) of the Commission Proposal, the official text explicitly states that, before the adoption of such delegated acts, the Commission shall carry out an impact assessment in accordance with Art. 56 CSA, with particular regard to paragraph 3[756]. Where no appropriate ECCS is available, the Commission may request ENISA to draft a candidate scheme[757].

In conclusion, the NIS2 considerably strengthens the level of cybersecurity in the Union and the IoT ecosystem would also benefit from the policy changes introduced by the revision of the NIS Directive. However, areas of uncertainty remain as to how the NIS2 legal framework will coordinate with the incoming Cyber Resilience Act which aims at laying down cybersecurity product requirements. In particular, section 3.5 has shown that bringing the manufacturing sector into the scope of the NIS2

---

[750] Art. 21(3) NIS2.

[751] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, OJ L 88, 29.03.2019, 42.

[752] BDI (n 733) 15; DIGITALEUROPE, 'DIGITALEUROPE Position on the NIS2 Directive' (n 733) 7.

[753] Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' (n 714) 13.

[754] Art. 24(1) NIS2.

[755] Art. 24(2) NIS2.

[756] DIGITALEUROPE, 'Reporting, Mandatory Certification and Main Establishment in Final NIS2 Trilogues' (2022) 3 <https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2022/05/DIGITALEUROPE_Reporting-Mandatory-Certification-Main-Establishment-in-final-NIS2-trilogues.pdf>.

[757] Art. 24(3) NIS2.

with new vulnerability handling procedures and supply chain cybersecurity requirements may create legal uncertainty.

3.6 The Cyber Resilience Act

3.6.1 A horizontal piece of legislation on cybersecurity for connected products

The Chapter has reviewed the EU legal frameworks addressing connected product cybersecurity, either directly or indirectly. The legislative gap analysis highlighted a fragmented regulatory landscape that does not specifically and comprehensively tackle the problem of unsecure connected products. In December 2021, the Commission published a "Study on the need of cybersecurity requirements for ICT products" (hereinafter 'the Study') which aimed to explore the current state of cybersecurity in broad categories of ICT products as well as to identify the reasons for the lack of sufficient security[758].

There are numerous problem drivers identified by the study underlying the lack of appropriate security in products with digital elements (Problem 1), together with an insufficient understanding among users of the level of cybersecurity of ICT products (Problem 2).

From a regulatory perspective, the sectoral approach adopted by the Commission vis-à-vis the inclusion of cybersecurity essential requirements in product safety legislation created legal uncertainty for both manufacturers and users while adding unnecessary burden on market operators to comply with overlapping requirements for similar types of products. From a market perspective, the failure to provide an optimal degree of cybersecurity has two main drivers i.e., information asymmetries and negative externalities. On the one hand, consumers are generally unable to assess the overall level of cybersecurity of digital products and may not be willing to pay for more secure options; on the other hand, several models analysing the optimal investment level in cybersecurity concluded that the cybersecurity market is characterised by a sub-optimal investment level[759].

Against this backdrop, in the 2021 State of the Union address EC President Von der Leyen announced a new 'Cyber Resilience Act' (CRA) to ensure a coherent cybersecurity framework with mandatory requirements for manufacturers of products with digital elements, building on the 2020 EU Cybersecurity Strategy for the Digital Decade, the Council Conclusions of 2 December 2020 and the Resolution of the European Parliament of 10 June 2021. The Commission then presented the proposal for a regulation on horizontal cybersecurity requirements for products with digital elements, already

[758] Wavestone - CEPS - CARSA - ICF (n 539).

[759] ibid 34–36.

amending Regulation (EU) 2019/1020 (Cyber Resilience Act) as of 15 September 2022. The legal basis of this legislative initiative was identified in Art. 114 of the Treaty on the Functioning of the European Union (TFEU), whose objective is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules.

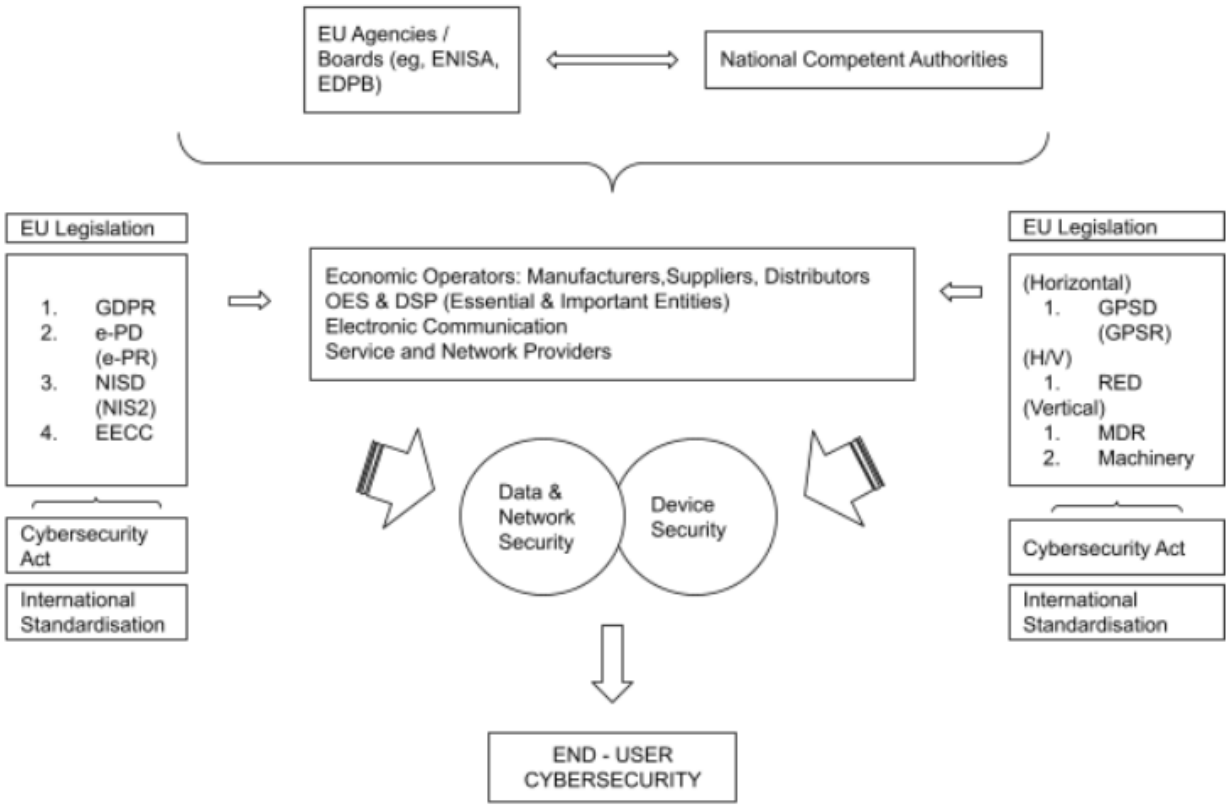


Figure 7: EU cybersecurity regulatory landscape pre-CRA. Source: the author.

3.6.2 Pillars of the Cyber Resilience Act proposal

3.6.2.1 The horizontal scope of the CRA

The CRA proposal applies "to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network"[760]. Whereas the EC call for evidence for an impact assessment used to refer to 'digital products and ancillary services'[761], the Proposal pivots on the concept of 'products with digital

[760] Art. 2(1) CRA Proposal.

[761] EU Commission, see <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en>.

elements' i.e., "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately"[762].

The scope of the Proposal is thus even broader than originally envisaged. The definition of 'products with digital elements' is a broad one in order to apply it to software as a separate product from hardware, as testified by the disjunctive use of the conjunction 'or'. The Reading of recital 46 of the Proposal seems to confirm this line of reasoning as it explicitly envisages products with digital elements in the form of software. Vast legal literature, especially in the area of civil liability, is devoted to the debate about whether software should be considered as a product[763]. This, however, will not be part of the analysis below. Instead, the extent to which the Proposal covers software-as-a-product need to be further investigated.

The explanatory memorandum of the CRA explicitly acknowledges that "current EU legal framework does not address the cybersecurity of non-embedded software"[764]. The chosen horizontal policy option intended to bring non-embedded software within its scope [765], with the only exception of software-as-a-service (SaaS). Nevertheless, Recital 9 of the Proposal specifies that the CRA may eventually also cover Software-as-a-Service (SaaS), "for remote data processing solutions *relating* to a product […] for which the software is designed and developed by the manufacturer of the product concerned or under the responsibility of that manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions". Therefore, to apply the CRA regime to SaaS, the 'relationship' of the software with the product for which it has been designed and developed for would appear to be decisive. In this respect, the 'ancillary' perspective of the early stages of the Cyber Resilience Act is somewhat restored. Finally, free and open-source software are excluded from the scope of the Proposal, in order not to hamper innovation or research[766].

Moreover, the CRA proposal would not cover products already falling within the scope of Regulation (EU) 2017/745 (Medical Devices Regulation)[767]; Regulation (EU) 2017/746 (Regulation on in vitro

---

[762] Art. 3(1) CRA Proposal.

[763] Gerhard Wagner, 'Software as a Product' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Smart Products: Münster Colloquia on EU Law and the Digital Economy VI* (Nomos Verlag 2022).

[764] Explanatory Memorandum to the CRA proposal, p. 1.

[765] ibid, p. 7.

[766] Recital 10 CRA Proposal.

[767] Whereas the CRA does not cover medical devices, it would cover devices that gather and process health data not falling under the scope of the MDR. See Richard Rak, 'Internet of Healthcare: Opportunities and Legal Challenges in Internet of Things-Enabled Telehealth Ecosystems' [2021] 14th International Conference on Theory and Practice of Electronic Governance (ICEGOV) 481, 483 <https://doi.org/10.1145/3494193.3494260> accessed 19 September 2022.: "with reference to Article 2(1) of the MDR, the threshold between a 'medical' and 'non-medical' device is the "intended purpose": whether the device is intended to be used by the manufacturer, alone or in combination, for one of the listed "specific medical purposes". The recent rise of consumer (well-being, lifestyle) health devices has blurred the borderline between 'medical' and 'non-medical' devices".

diagnostic medical devices); Regulation (EU) 2019/2144 (Automotive type-approval general regulation)[768], nor would it apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139 (Common rules in civil aviation)[769]. Products with digital elements exclusively developed for national security, military purposes or specifically designed to process classified information also fall outside the scope of the CRA proposal[770].

In line with the recent EU 'digital policies', the CRA proposal adopts a risk-based approach[771]. In relation to their level of cybersecurity risk, specific categories of products with digital elements can be classified as critical or highly critical if their core functionality falls into those categories[772]. In making these classifications, the Commission takes into account several criteria such as the cybersecurity-related functionality, intended use in sensitive environments or of performing critical functions and the extent of an adverse impact[773].

Critical products are further divided into class I[774] and class II[775], where class II represents a greater cybersecurity risk, and these are listed in Annex III to the CRA. The category of highly critical products can be created in the future by the Commission via delegated acts[776]. The different legal treatment of non-critical, critical and highly critical products with digital elements lies in the different conformity assessment procedure they have to comply with. On the one hand, critical products must undergo specific conformity assessment procedures referred to in Art. 24(2) and (3) CRA[777] (see Section 3.6.2.3). On the other hand, to demonstrate conformity with the essential requirements set out in Annex I, highly critical products must be certified under a European cybersecurity certification scheme[778].

3.6.2.2 The obligations for economic operators

With a view to ensuring effective cybersecurity along the entire supply chain (see in particular Section 1.4.4), the wide horizontal scope of the CRA proposal should be coupled with a set of obligations for

---

[768] Art. 2(2) CRA Proposal.

[769] Art. 2(3) CRA Proposal.

[770] Art. 2(5) CRA Proposal.

[771] Giovanni De Gregorio and Pietro Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59 Common Market Law Review 473.

[772] Art. 6(1) and 6(5) CRA Proposal.

[773] Art. 6(2) CRA Proposal.

[774] This class of products includes *inter alia* identity management systems software and privileged access management software password managers, network traffic monitoring systems, SIEM systems.

[775] This class of products includes *inter alia* operating systems, public key infrastructure and digital certificate issuers, firewalls, intrusion detection systems, general purpose microprocessors.

[776] Art. 6(5) CRA Proposal.

[777] Art. 6(4) CRA Proposal.

[778] Art. 6(5) CRA Proposal.

all the economic operators involved: from manufacturers up to distributors and importers, adequate for their responsibilities on the supply chain, a wide array of stakeholders will have to comply with the new set of rules. In this respect, the new approach in EU cybersecurity law of including the entire value chain of products with digital elements within scope should be pointed out. Traditionally, relationships between economic operators along the supply chain have primarily been contractual. The CRA proposal designs a novel approach in EU cybersecurity law insofar as the law will now require manufacturers to exercise due diligence when integrating components sourced from third parties in products with digital elements[779].

On a general level, three main conditions apply for the placing on the market of products with digital elements:

i) they shall be properly installed, maintained, used for their intended purpose and, where applicable, updated[780];
ii) they shall be designed, developed and produced in accordance with the essential requirements laid down in Section 1 of Annex I[781];
iii) the processes put in place by the manufacturer shall comply with the essential requirements set out in Section 2 of Annex I[782].

The essential requirements set out in Section 1, Annex I relate to the properties of products with digital elements. *Inter alia*, products shall be designed, developed and produced to ensure an appropriate level of cybersecurity based on the risks; shall be delivered without any known exploitable vulnerabilities; shall be delivered with a secure by default configuration; shall ensure protection from unauthorised access by appropriate control mechanisms; shall protect the confidentiality of processed personal or other data by means of state-of-the-art encryption; etc.

On the other hand, the essential requirements laid down by Section 2, Annex I focus on the processes put in place by manufactures, in particular, taking into account the handling of vulnerabilities. Therefore, manufacturers will: identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product; address and remediate vulnerabilities without delay, including by providing security updates; apply effective and regular tests and reviews of the security of the product; publicly disclose information about fixed vulnerabilities, once a security update has been made available, etc.

---

[779] Art. 10(4) CRA Proposal.

[780] Art. 5, point (1) CRA Proposal.

[781] Art. 10(1); Art. 5, point (1) CRA Proposal.

[782] Art. 5, point (2) CRA Proposal.

With a view to complying with the obligation to place a product on the market in accordance with the essential requirements of Section 1, Annex I, manufacturers shall undertake an assessment of the cybersecurity risks related to a product category. The outcome of the risk assessment must be taken into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements[783]. The risk assessment shall be included in the technical documentation as set out in Art. 23 and Annex V[784].

Manufacturers also have several documentation obligations with regard to relevant cybersecurity aspects of the product. These are handling vulnerabilities, information provided by third parties and the update of the risk assessment[785]. In this respect, Art. 23 specifies that the content of the technical documentation must be drawn up by the manufacturer before the product is placed on the market and must be kept at the disposal of the market surveillance authorities for ten years after the product has been placed on the market[786].

With regard to the cooperation duties with market authorities (see Section 3.6.2.4), manufacturers must also: i) provide that authority with all the information necessary to demonstrate conformity with Annex I essential requirements, and cooperate on any measurers taken to eliminate the cybersecurity risks posed by the product[787]; ii) inform the authority about the cessation of its operations with the consequence of not being able to comply with the obligations of the Regulation[788].

Moreover, manufacturers will ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form, in a clear, understandable, intelligible and legible language[789]. The instructions and information may include the EU declaration of conformity[790].

The CRA proposal also lays down reporting obligations for manufacturers and adopts a *quasi*-centralised approach. In fact, manufacturers notify ENISA of any actively exploited vulnerability contained in the product, including the details and any mitigating measures taken[791], and any incident having impact on the security of the product with digital elements[792], without undue delay and in any event within 24 hours of becoming aware of it. In turn, ENISA forwards the notification to the CSIRT

[783] Art. 10(2) CRA Proposal.
[784] Art. 10(3) CRA Proposal.
[785] Art. 10(5) CRA Proposal.
[786] Art. 10(8) CRA Proposal.
[787] Art. 10(13) CRA Proposal.
[788] Art. 10(14) CRA Proposal.
[789] Art. 10(10) CRA Proposal.
[790] Art. 10(11) CRA Proposal.
[791] Art. 11(1) CRA Proposal.
[792] Art. 11(2) CRA Proposal.

designated for the purposes of coordinated vulnerability disclosure or to the single point of contact under the NIS2 framework, depending on whether the notification regards a vulnerability or an incident, without undue delay, unless for justified cybersecurity risk-related grounds[793].

Manufacturers also have to inform the product users about corrective measures to be deployed to mitigate the impact of the incident[794], and the person or entity maintaining the component – integrated in the product – affected by a vulnerability identified by the manufacturer[795].

Lastly, Articles 12, 13 and 14 place obligations on the other economic operators in the supply chain beside manufacturers i.e., authorised representatives, importers and distributors. It shall be noted that if importers or distributors place a product on the market under their name or trademark or carry out a substantial modification of the product[796], they will then be considered a manufacturer. Therefore, they will be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7)[797]. Importantly, the same applies to any natural or legal person who carries out a substantial modification.

3.6.2.3 Essential cybersecurity requirements and conformity assessment

The CRA proposal builds on the existing setting of the NLF legislation, with its structures and procedures. In particular, Art. 18 of the CRA proposal regulates the presumption of conformity with the Regulation. Products and processes in conformity with harmonised standards, or parts thereof, the references of which have been published in the *Official Journal of the European Union*, and EU statement of conformity or certificate issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 will be presumed to conform with the essential requirements of the Cyber Resilience Act. With regard to the latter, the Commission may use implementing acts to specify the schemes that can be used to demonstrate conformity with the essential requirements of Annex I CRA and whether a cybersecurity certificate eliminates a manufacturer's obligation to carry out a third-party conformity assessment for the corresponding requirements[798].

---

[793] Sandra Schmitz and Stefan Schiffner, 'Responsible Vulnerability Disclosure under the NIS 2.0 Proposal' (2021) 12 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 448 <https://www.jipitec.eu/issues/jipitec-12-5-2021/5495>.

[794] Art. 11(4) CRA Proposal.

[795] Art. 11(7) CRA Proposal.

[796] According to Art. 3, point (31) CRA, 'substantial modification' "means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed".

[797] Art. 15 CRA Proposal.

[798] Art. 18(4) CRA Proposal.

If harmonised standards do not exist, are insufficient or if there are undue delays in the standardisation procedure or the Commission request has not been accepted by the ESOs, the Commission may, by means of implementing acts, adopt common specifications[799] that can be used to demonstrate conformity with the essential requirements of Annex I, to the extent those common specifications cover those requirements[800].

The EU declaration of conformity, stating that fulfilment of the applicable essential requirements set out in Annex I has been demonstrated, will be drawn up by manufacturers in accordance with the documentation duties of Art. 10(7)[801]. Annex IV contains the model structure of the EU declaration of conformity which: i) must contain the elements specified in the relevant conformity assessment procedures set out in Annex VI[802]; ii) shall be continuously updated[803]; iii) if a product with digital elements is subject to more than one Union act requiring an EU declaration of conformity, it shall contain the identification of the Union acts concerned[804].

As already mentioned in the previous section, the compliance of critical products is limited either to the EU-type examination procedure (based on module B) followed by conformity to the EU-type based on internal production control (based on module C) or to conformity assessment based on full quality assurance (based on module H)[805]. With regard to the categories of critical products belonging to class I, manufacturers must adhere to said procedures only *if* they have not applied or *have only applied in part* harmonised standards, common specifications or European cybersecurity certification schemes; or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist[806].

The CE marking shall be affixed visibly, legibly and indelibly to the product before placing the product with digital elements on the market [807]. Economic operators shall follow the general NLF principles set out in Article 30 of Regulation (EC) No 765/2008[808].

---

[799] Art. 19 CRA Proposal.

[800] Art. 18(2) CRA Proposal.

[801] Art. 20(1) CRA Proposal.

[802] These include: (a) the internal control procedure (based on module A of Decision 768/2008/EC); or (b) the EU-type examination procedure (based on module B) followed by conformity to EU-type based on internal production control (based on module C); or (c) conformity assessment based on full quality assurance (based on module H).

[803] Art. 20(2) CRA Proposal.

[804] Art. 20(3) CRA Proposal.

[805] Art. 24(2) and (3) CRA Proposal.

[806] Art. 24(2) CRA Proposal.

[807] Art. 22(1) CRA Proposal. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 20 or on the website accompanying the software product.

[808] Art. 21 CRA Proposal.

Finally, the CRA proposal sets out the rules regulating the interactions with national conformity assessment bodies (notified bodies). Consistently with NLF principles, Member States must designate a notifying authority that will be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and monitoring of notified bodies[809].

3.6.2.4 Market surveillance

Member states must designate national market surveillance authorities (MSAs) that carry out market surveillance. For the purpose of ensuring the effective implementation of the CRA, national authorities can be any existing or new authority, including national competent authorities under the NIS2 and the Cybersecurity Act (CSA)[810]. Against this backdrop, Eurosmart suggests granting market surveillance powers to national cybersecurity certification authorities (NCCAs) under the Cybersecurity Act, provided that: i) these public authorities already have the capability and necessary expertise in the cybersecurity field; ii) NCCAs have been designated and have the relevant knowledge to supervise the NLF's Conformity Assessment Bodies[811]. As an exception, the MSAs designated for the purposes of the Artificial Intelligence Act (AIA) will be the authorities responsible for market surveillance activities required under the CRA for products with digital elements which are classified as well as high-risk AI systems according to the AIA [812].

Beyond the current rules for market surveillance contained in the NLF, and specifically in Regulation (EU) 2019/1020 – which applies to the products with digital elements within the scope of the CRA[813], since cybersecurity must be guaranteed through the entire lifecycle of products with digital elements, it has been deemed necessary "to extend the post-market surveillance activity to guarantee the security of product during the usage phase and when the products are removed from the market"[814].

MSAs established to ensure the effective implementation of the CRA shall cooperate with: i) other market surveillance authorities designated on the basis of other Union harmonisation legislation; ii) national cybersecurity certification authorities designated under the CSA; and, iii) as appropriate, with data protection authorities. BEUC explicitly called for cooperation mechanisms between national authorities and consumer protection organisation "to create synergies towards a better market

---

[809] Art. 26 CRA Proposal.

[810] Recital 55 CRA Proposal.

[811] Eurosmart, 'Cyber Resilience Act (CRA) - New Cybersecurity Rules for Digital Products and Ancillary Services' (2022) 9–10 <https://www.eurosmart.com/cyber-resilience-act-cra-new-cybersecurity-rules-for-digital-products-and-ancillary-services/>.

[812] Art. 41(10) CRA Proposal.

[813] Art. 41 CRA Proposal.

[814] Wavestone - CEPS - CARSA - ICF (n 539) 196.

screening, raising awareness and prevent violations of CRA obligations"[815]. In this regard, different MSAs can carry out joint activities. These cooperative powers can be triggered by the Commission or ENISA, with the aim of ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed or made available on the market[816]. Among these actions are the so-called 'sweeps' i.e., simultaneous coordinated control actions of products with digital elements, or categories thereof, to check compliance with or to detect infringements to the CRA[817]. Sweeps are coordinated by the Commission, unless otherwise decided by the MSAs conducting the action.

On an annual basis, MSAs report the outcomes of relevant market surveillance activities that have been carried out to the Commission. They include evaluations of products in respect of their compliance with the CRA's essential requirements, if the authority has sufficient reasons to consider that the products concerned present a significant cybersecurity risk[818]. Where a product is found not comply with relevant CRA provisions, the MSA requires the economic operator to take all appropriate corrective actions to bring the product into compliance with those requirements without delay, to withdraw it from the market, or to recall it within a reasonable period[819]. If the manufacturer does not take the adequate corrective actions within the timeframe given by the MSA, the authority takes action to prohibit or restrict that product being made available on its national market, to withdraw it from that market or to recall it[820]. The Commission is empowered to initiate these evaluations and, if there are reasons to consider that no effective measures have been taken by the relevant market surveillance authorities, to request ENISA to carry out an evaluation of compliance *in lieu* of the MSA concerned[821]. Corrective or restrictive actions may be adopted by the Commission at Union level by implementing acts accordingly.

In terms of sanctions, the CRA proposal leaves the responsibility to set rules on effective, proportionate and dissuasive penalties applicable to infringements of the CRA to the Member States[822]. However, the discretion of Member States in setting up the framework on penalties is constrained by the Proposal. Firstly, non-compliance with the essential cybersecurity requirements of

---

[815] BEUC, 'Cyber Resilience Act: Cybersecurity of Digital Products and Ancillary Services - BEUC Response to Public Consultation' (2022) 11 <https://www.beuc.eu/publications/beuc-x-2022-051_cyber_resilience_act_public_consultation_beuc_position_paper.pdf>.

[816] Art. 48 CRA Proposal.

[817] Art. 49 CRA Proposal.

[818] Art. 43(1) CRA Proposal.

[819] *Ibidem.*

[820] Art. 43(4) CRA Proposal.

[821] Art. 45 CRA Proposal.

[822] Art. 53(1) CRA Proposal.

Annex I and the obligations set out in Articles 10 and 11 will be subject to administrative fines of up to 15 million EUR or, if the offender is an undertaking, up to 2.5 % of its total worldwide annual turnover for the preceding financial year, whichever is higher [823]. Secondly, non-compliance with any other obligations under this Regulation will be subject to administrative fines of up to 10 million EUR or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover[824]. Lastly, supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request will be subject to administrative fines of up to 5 million EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover[825]. Member States must notify the Commission of the implemented rules and measures without undue delay[826].

To be effective in cybersecurity, market surveillance needs not only dissuasive sanctions[827], but also necessary competences. "This is especially the case because of the important role that processes play in cybersecurity, going beyond the traditional product-based expertise of market surveillance authorities and the global nature of such processes and products"[828]. To this end, it will be vital that MSAs enforcing the CRA are equipped with adequate resources [829].

3.6.3 Interplay with other Union policies

The 'horizontal legislation' policy option as it has been presented in this section needs to be streamlined and aligned with the most recent initiatives undertaken by the EC to close some gaps with regard to the cybersecurity of digital products, as addressed in this Chapter. In particular, the attention focuses on the RED Delegated Regulation 2022/30, the General Product Safety Regulation (GPSR) proposal, the Machinery Regulation (MR) proposal, the Medical Devices Regulation (MDR), the Cybersecurity Act and the NIS2.

3.6.3.1 Interplay between the CRA and the General Product Safety Regulation Proposal

Article 7 of the CRA proposal functions as an interface between the CRA and the General Product Safety Regulation which, as seen in Section 3.4.3, would apply as *lex generalis* to non-harmonised

---

[823] Art. 53(3) CRA Proposal.

[824] Art. 53(4) CRA Proposal.

[825] Art. 53(5) CRA Proposal.

[826] Art. 53(2) CRA Proposal.

[827] ANEC, 'ANEC Response to EC Call for Evidence for an Impact Assessment on the Cyber Resilience Act (CRA) Initiative' (2022) 6 <https://www.anec.eu/images/Publications/position-papers/Digital/ANEC-2022-DIGITAL-CYBER-006.pdf>; Bitkom, 'Cyber Resilience Act (CRA)' (2022) 4 <https://www.bitkom.org/EN/List-and-detailpages/Publications/Position-Paper-Cyber-Resilience-Act>.

[828] DIGITALEUROPE, 'Building Blocks for a Scalable Cyber Resilience Act' (2022) 13 <https://www.digitaleurope.org/wp/wp-content/uploads/2022/05/Building-blocks-for-a-scalable-Cyber-Resilience-Act.pdf>.

[829] Sandra Schmitz-berndt and Pier Giorgio Chiara, 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive' [2022] International Cybersecurity Law Review 14.

products and to the harmonised consumer products for the aspects that are not covered by harmonised legislation. Art. 7 CRA reads as follows:

> "*By way of derogation from Article 2(1), third subparagraph, point (b), of Regulation [General Product Safety Regulation] where products with digital elements are not subject to specific requirements laid down in other Union harmonisation legislation within the meaning of [Article 3, point (25) of the General Product Safety Regulation], Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation [General Product Safety Regulation] shall apply to those products with respect to safety risks not covered by this Regulation*".

Recital 28 CRA, read in conjunction with the relevant articles of the GPSR, should shed light on the meaning of the provision. In fact, Recital 28 acknowledges that products under the CRA scope may pose safety risks that are not cybersecurity- related. Such risks are already regulated by other EU legal acts within product safety *acquis*. It follows that if no other harmonised Union legislation is applicable, the GPSR legal framework would come into play, in accordance with its function of a 'safety net'. However, Article 2(1) GPSR states that where products are within the scope of Union product safety legislation, the rules laid down by the GPSR shall apply only to the aspects and risks not covered by those requirements; in particular, Chapter III, Section 1, Chapters V and VII, Chapters IX to XI GPSR shall not apply.

Therefore, the derogation found in Art. 7 CRA from the general rule mandated by Art. 2(1) GPSR finds its rationale in the targeted nature of the Cyber Resilience Act. Thus, the CRA only covers cybersecurity-related aspects without addressing more general health and safety requirements as the legal acts of EU product legislation. Consequently, extending the coverage of Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI GPSR to products with digital elements with respect to safety risks not covered by the CRA should be seen in a fundamentally positive light.

3.6.3.2 Interplay between the CRA and the Machinery Regulation Proposal

Similarly, Art. 9 CRA proposal regulates the interface between the Cyber Resilience Act and the Machinery Regulation proposal. In particular, it specifically fleshes out the interplay between the conformity assessments under the two pieces of legislation. Where machinery products are also products with digital elements within the meaning of the CRA and for which an EU declaration of conformity has been issued on the basis of the CRA, they will be deemed to be in conformity with the essential health and safety requirements set out in Annex III, Sections 1.1.9 and 1.2.1 to the Machinery Regulation proposal, as addressed in Section 3.4.5.

3.6.3.3 Interplay between the CRA and the RED Delegated Act

The CRA proposal explicitly acknowledges that the essential requirements set out in Annex 1 CRA include all the elements of the essential requirements referred to in Article 3(3) points (d), (e) and (f) of the RED[830]. Furthermore, CRA's essential requirements are also aligned "with the objectives of the requirements for specific harmonised standards included in the standardisation request" of the Commission to the European Standardisation Organisations to prove conformity with the RED's above-mentioned requirements[831].

Following the line of reasoning of recital 15 CRA, the so-called 'RED Delegated Act' (see Section 3.4.2) completely overlap, either in terms of content or objectives, with the CRA Proposal. Thus, the CRA proposal explicitly considers repealing or amending Delegated Regulation (EU) 2022/30. In such case, the Commission and ESOs "should take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on a standardisation request for the RED Delegated Regulation 2022/30 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation"[832].

3.6.3.4 Interplay between the CRA and the NIS2 Directive

Three main areas of interplay are considered in this section, mirroring the ones taken into account in the analysis of the NIS2 (Section 3.5). They regard: i) the scope of the legal acts; ii) the rules regulating supply chain relationships; iii) the reporting of incidents and vulnerabilities.

First, the NIS2 will complement the CRA by bringing into scope cloud computing services and cloud service models, such as SaaS[833]. Further, a criterion that shall be taken into account by the Commission when determining the categories of highly critical products is the fact that a category of products with digital elements is used or relied upon by the essential entities within the meaning of NIS2 or will have potential future significance for the activities of these entities.

Second, the CRA will complement the NIS framework by ensuring the preconditions for strengthening supply chain cybersecurity[834]. Thus, complying with the supply chain cybersecurity requirements under Articles 21(2)(d), 21(3) and 22 of the NIS2 would be eased by the set of obligations introduced by the CRA: the latter will ensure that the digital products used by essential and important entities for the provision of their services are designed and manufactured according to

---

[830] Recital 15 CRA Proposal

[831] *Ibidem*.

[832] *Ibidem*.

[833] Recital 9 CRA Proposal.

[834] Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' (n 713) 12; Explanatory Memorandum to the CRA Proposal, p. 7.

state-of-the-art cybersecurity controls. Also, the dynamic and life-cycle approach of the CRA would guarantee that NIS2 entities have access to timely security updates for the products concerned[835].

A third area of intersection consists of reporting duties. As seen in Section 3.6.2.2, manufacturers of products with digital elements primarily have reporting obligations in terms of actively exploited vulnerabilities and incidents that have impact on the security of the product (Art. 11 CRA). The *quasi*-centralised model of governance introduced by the CRA proposal places ENISA at the core of the notification system's procedural framework. On the one hand, an efficient and timely communication between ENISA and the single point of contact of the Member States concerned, with respect to the incidents[836], and the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Art. 12 of the NIS2[837] should be ensured. On the other hand, it will be crucial to avoid conflicts and overlaps with the incidents and vulnerabilities reporting duties of essential and important entities under the NIS2, in order not to create legal confusion.

3.6.3.5 Interplay between the CRA and the Cybersecurity Act

The CRA proposal aims to exploit synergies with the Cybersecurity Act mainly with regard to the conformity assessment procedure. Art. 18(3) and (4) CRA lay down the interface between the two legal frameworks with a view to promoting the European cybersecurity certification schemes (ECCS) and facilitating the assessment of conformity of products with digital elements – if covered by an EU statement of conformity or certificate under a ECCS pursuant to Regulation (EU) 2019/881.

The Commission may specify the ECCSs that can be used for the presumption of conformity with CRA's essential requirements through the adoption of implementing acts, and if a cybersecurity certificate issued under such schemes eliminates a manufacturer's obligation to carry out a third-party conformity assessment for the corresponding requirements[838]. The Commission is also empowered to adopt delegated acts to specify the categories of highly critical products for which manufacturers will be required to obtain a certificate under an ECCS to demonstrate conformity with the essential requirements set out in the CRA[839].

Finally, the CRA Proposal seemingly retains a benchmark role in respect to future ECCSs: "the need for new European cybersecurity certification schemes for products with digital elements should be assessed in the light of this Regulation. Such future European cybersecurity certification schemes

[835] Recital 11 CRA Proposal.

[836] Art. 11(1) CRA Proposal.

[837] Art. 11(2) CRA Proposal.

[838] Art. 18(4) CRA Proposal.

[839] Art. 6(5) CRA Proposal.

covering products with digital elements should take into account the essential requirements as set out in this Regulation and facilitate compliance with this Regulation"[840].

3.7 Conclusion

This Chapter charted the different pieces of EU legislation in the field of cybersecurity to investigate the extent to which they tackle the specific security challenges raised by IoT connected devices. In other words, whether existing and proposed EU cybersecurity legal frameworks address the problem of unsecure digital connected devices.

The NIS Directive, the first EU legal instrument in the cybersecurity acquis, covers both governance (i.e., Member States obligations in terms of cybersecurity strategies, establishing CSIRTs, point of contacts, etc.) and procedural cybersecurity aspects in terms of incidents and risk management measurers for the sole operators of essential services and digital service providers. Albeit the Directive enhanced the overall security of key economic sectors within the Union, it did not target IoT products specifically, as described in the legal analysis. Even the Proposal for a NIS2, which considerably strengthens the level of protection offered by the NIS Directive to the IoT ecosystem, would only cover the connected devices forming part of the network and information systems of EE and IE by the scope *rationae personae* of the NIS 2.

Therefore, the analysis looked at the EU cybersecurity certification framework introduced by the Cybersecurity Act as a means to address the problem under scrutiny. By focusing in particular on the comprehensive security objectives for the EU cybersecurity schemes, laid down by Art. 51, it might seem that this legal framework can cope with the lack of 'strong' cybersecurity of connected products in the Single Market. However, recourse to EU cybersecurity certification is voluntary. The analysis therefore demonstrated that depicting the CSA framework as *purely* voluntary is rather inaccurate. Firstly, the CSA explicitly foresees the possibility of imposing specific cybersecurity requirements and making the certification thereof mandatory. Secondly, Member State or other Union law can provide for legally binding schemes, as confirmed in Article 21 of the Proposal for NIS2. Finally, incentives towards certification may come from the market, as most of the customers and vendors along the supply chain look for certified products, services and processes, even at higher costs.

At the same time, the Commission – pressured by a surge in cyberattacks, both in terms of quality and quantity – took action by following a 'vertical' approach: it embarked on the revision of product

[840] Recital 39 CRA Proposal.

safety legislation with the view to including cybersecurity requirements. The investigation showed to what extent the RED, and in particular the Delegated Act activating Article 3(3)(d), (e), and (f), the MDR, the Proposal for a Regulation on General Product Safety and on Machinery Equipment address the above-mentioned regulatory failures.

In conclusion, this Chapter highlighted that while a vertical approach might be effective in the short run, only horizontal legislation will efficiently address the problem of the lack of legal obligations for the manufacturers of connected devices vis-à-vis the cybersecurity of their digital solutions at the core.

The Cyber Resilience Act proposal introduces a set of ex-ante and ex-post obligations impacting all the economic operators along the supply chain about the cybersecurity of their products with digital elements. Moreover, this policy option would address the second negative externality arising from the application of a theory of public good to the cybersecurity's dimension of robustness (section 2.2.3): the costs of the failures will be borne by producers and will no longer fall on end users. The explanatory memorandum to the CRA proposal seems to share this line of reasoning stating that "any compliance costs for businesses would be outweighed by the benefits brought by a higher level of security of products with digital elements and ultimately an increase of users' trust in these products"[841]. With regard to the added costs in terms of compliance, in order not to overly burden economic operators, notified bodies should set conformity assessment fees proportional to the size of the undertaking. On the other hand, the horizontal policy option adopted would also bring significant benefits to the stakeholders involved: "for businesses, it would prevent divergent security rules for products with digital elements and decrease compliance costs for related cybersecurity legislation. It would reduce the number of cyber incidents, incident handling costs and reputational damage"[842]. Yet, the EU Parliament and the Council are now called on to work on the CRA proposal in the trilogue with a view to harmonising a fragmented regulatory landscape and avoiding overlaps or, worse, conflicts between the various requirements from different pieces of legislation.

[841] Explanatory Memorandum to the CRA Proposal, p. 5.

[842] Legislative financial statement to the CRA Proposal, p. 69.

Chapter 4. Privacy and Data Protection Challenges in IoT Data and Metadata Processing

4.1 The Interplay between EU Privacy and Data Protection Legal Frameworks concerning IoT Data and Metadata Processing and Sharing

When it comes to mapping the *privacy* debate on the Internet of Things, it is often hard to discern issues relating to the right to privacy from the ones relating to the right of data protection (for a functional definition of 'privacy', see Chapter 2, section 2.2.1). Indeed, the "technical literature" – understood as the research corpus that has not been shaped by legal scholars – tends to acknowledge 'privacy' in a broad and holistic fashion, that is, to include *privacy-as-confidentiality* and *informational privacy* (see Chapter 2), with the latter including data protection related concerns, without making a due and appropriate division.

In this respect, Konoudes and Kapitsaki carried out a systematic literature review to identify the state-of-the-art of scientific research vis-à-vis user's privacy protection in the IoT: out of 84 papers analysed, 58 contain the word "privacy" in the title, whilst only 6 include "personal data" or "data protection"[843]. Unsurprisingly, all the contributions examined by the authors tackle several challenges brought about by the IoT in terms of applying GDPR[844] requirements. Albeit some may see this problematisation as a merely formalistic exercise, this trend, which arguably has its roots in a more US-minded reconstruction of privacy frameworks and values[845], conceals deeper consequences, as the incorrect framing of the problem will be reflected in a negative legacy at legal level.

---

[843] Alexia Dini Kounoudes and Georgia M Kapitsaki, 'A Mapping of IoT User-Centric Privacy Preserving Approaches to the GDPR' (2020) 11 Internet of Things.

[844] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[845] Jeroen van den Hoven and others, 'Privacy and Information Technology' in Edward N Zalta (ed), *Stanford Encyclopedia of Philosophy* (Stanford University Press 2020): the European approach "conceptualises issues of informational privacy in terms of data protection", whilst US scholars in terms of privacy.

Against this background, without dwelling on classifications of privacy theories[846], this section aims to highlight how structural IoT data and metadata harvesting, processing and sharing (see Chapter 1) trigger and challenge specific aspects of the relevant EU privacy and data protection legal frameworks i.e., the GDPR and ePrivacy laws[847], in order to include the drafts of the ePrivacy Regulation[848], proposed by the Commission in January 2017[849], in the legal analysis. Notwithstanding other considerations suggesting a (re)alignment between privacy and data protection under the IoT paradigm[850], several legal challenges facing both the GDPR and ePrivacy laws are also scrutinised: i) lawfulness of IoT data and metadata processing, in particular, taking into account the effectiveness of relying on 'consent' as a legal basis; ii) lack of control and information asymmetry, with due regard for the principle of transparency; iii) information security risks, as opposed to device or network security, addressed in Chapter 3.

The three above-mentioned issues were identified by the Article 29 Working Party in its 2014 Opinion on the recent developments of the Internet of Things[851]. Drawing on the findings of the Opinion, the analysis that follows aims to enrich the theoretical reflection by taking into account recent developments either at technological (e.g., innovative tracking techniques) or legislative (i.e., the ePrivacy Regulation Proposal) level. Some other risks identified by the Article 29 WP (i.e., profiling; limits of anonymisation; inferences derived from data) are seemingly left out of the discussion. However, given the fact that they can be considered different facets of the same problem, namely IoT data and metadata analysis, they will be dealt with in a unified and more comprehensive way by the remaining sections of this chapter.

It may be worth clarifying from the outset the difference between data and metadata. From an epistemological perspective, 'content data' present traits of subjective interpretation, whereas 'content metadata' are more meaningful and objective as they regard the time, the date, the source,

---

[846] Bert-jaap Koops and others, 'A Typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483; Daniel J Solove, *Understanding Privacy* (Harvard University Press 2010).

[847] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[848] European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final.

[849] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, ePrivacy Regulation) COM/2017/010 final.

[850] Pagallo, Durante and Monteleone (n 77) 59.

[851] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (2014) <http://ec.europa.eu/justice/data-protection/index_en.htm> accessed 31 January 2020.

the destination and the length fields of the communication[852]. In this respect, metadata set the context in which the content of the communication is formed and shared. Many scholars agree that a sharp separation, or rather discrimination, in terms of legal protection between data and metadata, following an outdated 'content – envelope' metaphor, would be detrimental in two respects. First, there is no dispute that metadata are no less sensitive than content data[853]. Secondly, the boundaries between content and metadata, in network communication, are increasingly blurred[854]. A relativistic or contextual approach to distinguish between content and metadata considers the specific circumstances in which the information is formed or used: for example, a URL is at the same time a "delivery instruction", that is, metadata, and content since "essentially means sending a message saying «please send me back the page found at this URL»"[855].

On a more general level, the e-Privacy Directive – as amended by Directive 2009/136/EC[856] – seeks to harmonise national provisions to uphold fundamental rights and freedoms, in particular, the right to privacy (Art. 7 EU Charter of Fundamental Rights), intended in the sense of *confidentiality*, with respect to the specific electronic communication sector[857], which may involve the processing of personal, non-personal data and data related to a legal person[858]. Conversely, the GDPR protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data[859], horizontally, without restricting its scope to a particular (vertical) sector. As Poletti rightly noticed, "the IoT stands at the crossroads between these two coordinates, revealing that through the network of connected sensors, injuries to both rights can be generated; […] it can be said

---

[852] Palmirani and Martoni (n 8) 9–22.

[853] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, judgment of 21 December 2016 (Grand Chamber), ECLI:EU:C:2016:970, para. 99.

[854] Lilian Mitrou, 'Communications Data Retention: A Pandora's Box for Rights and Liberties?' in Alessandro Acquisti and others (eds), *Digital Privacy: Theory, Technologies, and Practices* (Auerbach Publications 2007) 422. See also See also Opinion of Advocate General Bobek, Case of 26 January 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:43, para. 95.

[855] Chris Conley, 'Metadata: Piecing Together a Privacy Solution' (2014) 4–5 <https://www.aclunc.org/sites/default/files/Metadata report FINAL 2 21 14 cover %2B inside for web %283%29.pdf>.

[856] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] GJ L 337/11

[857] Art. 1(1) ePD.

[858] Art. 1(3) ePD.

[859] Art. 1(2) GDPR.

that the IoT is now positioned in the middle between the GDPR, which does not properly fit this infrastructure, and Directive 2002/58/EC"[860].

The e-Privacy Regulation aims to revise an outdated Directive, which is no longer coherent[861] and therefore fit for the increasing digitalised Single Market and, more generally, society and providing a level playing field for market players[862]. In its Proposal, the Commission broadened the material and territorial[863] scope of the previous Directive. The Regulation, as drafted by the Commission, would apply to "the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users" (Art. 2(1)), whereas the electronic communications services that are not publicly available would fall outside the scope (Art. 2(2)(c)).

It follows that the new legal act would cover not only traditional telecom providers but also 'over-the-top' (OTT) players[864], such as providers of voice over IP, text message and email services[865]. In this respect, both the Parliament[866] and Council[867] drafted legislative resolutions on the Commission's Proposal amended Art. 2 so to include the 'provision of publicly available directories' and the 'sending of direct marketing electronic communications'. In particular, the Parliament extended the scope of the Regulation to include information processed (not just stored) by end-users terminal equipment and the placing on the market of software permitting electronic communications. Finally, one significant source of friction between the co-legislators is whether the Regulation should apply to electronic communications data and metadata *stored* or, rather, only *in transit.* Whereas the Council

---

[860] Dianora Poletti, 'IoT and Privacy' in Roberto Senigaglia, Claudia Irti and Alessandro Bernes (eds), *Privacy and Data Protection in Software Services* (2022) Springer, 178.

[861] Christina Etteldorf, 'A New Wind in the Sails of the EU Eprivacy-Regulation or Hot Air Only? On an Updated Input from the Council of the EU under German Presidency' (2020) 6 European Data Protection Law Review 4, 568.

[862] European Commission, 'Explanatory Memorandum of the Proposal for the ePrivacy Regulation' (2017) 2; recital 6, ePrivacy Regulation.

[863] Similar to the GDPR, the provisions of the ePrivacy Regulation would have an extraterritorial effect, as they would apply to the processing of electronic communications content, metadata and the information related to the terminal equipment of end-users in the Union (Art. 3).

[864] Body of European Regulators for Electronic Communication, 'Report on OTT Services' (2016) <https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5751-berec-report-on-ott-services_0.pdf>.

[865] Elena Gil González, Paul De Hert and Vagelis Papakonstantinou, 'The Proposed EPrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads?' in Dara Hallinan and others (eds), *Data Protection and Privacy: Data Protection and Democracy* (Hart Publishing 2020) 256–257.

[866] European Parliament, 'Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM(2017) <https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html> accessed 18 March 2022.

[867] Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (2021) <https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf> accessed 10 March 2022.

explicitly supports the latter interpretation[868], Parliament amends Recital 15 by adopting an absolutist stance towards the prohibition of interception of communications, whether in transit or stored[869].

Importantly, Recital 12 highlights the need to ensure full protection of the rights to privacy and confidentiality of machine-to-machine communications and Internet of Things services, unless IoT transmission is carried out via a private or closed network such as a closed factory network. However, the Commission Proposal does not substantiate this recital in any article. Conversely, Parliament amended the definition of 'electronic communications service' to include "a service consisting wholly or mainly in the conveyance of the signals, such as a transmission service used for the provision of a machine-to-machine service and for broadcasting, but excludes information conveyed as part of a broadcasting service to the public over an electronic communications network or service except to the extent that the information can be related to the identifiable end-user receiving the information; it also includes services which are not publicly available, but provide access to a publicly available electronic communications network"[870].

The words used by the Parliament to describe the M2M interaction, and the Internet of Things in general i.e., 'conveyance of the signals', echoes the phrasing of Art. 2(4)(c) of the European Electronic Communications Code[871] (see Chapter 3, section 3.2.1.1). While the Parliament[872] and some commentators highlight the risk of relying on another legal instrument when providing definitions[873], the overall consistency effort between Union acts is positive as it ensures legal certainty and coherence.

The Article 29 Working Party, while welcoming the expansion of the scope to cover M2M interaction – "as such communications often contain information protected under privacy rights", argued, on the other hand, that "a narrow category of *pure* [emphasis added] machine-to-machine communication should be exempted if they have no impact on either privacy or the confidentiality of communications, such as for example the cases where such communication is performed in execution of a transmission protocol between network elements (e.g. servers, switches,) to inform each other on their status of

---

[868] Art. 2(2)(e) Council ePrivacy Proposal: [The Regulation does not apply to] electronic communications data processed after receipt by the end-user concerned.

[869] In the Parliament's reading, the new version of recital 15 states that "prohibition of interception of communications should apply *also* during their conveyance [emphasis added]".

[870] Art. 4(3)(aa) Parliament ePrivacy Proposal.

[871] DIRECTIVE (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

[872] Art. 4(3)(aa, ab, ac, ad, ae, af) Parliament ePrivacy Proposal.

[873] González, Hert and Papakonstantinou (n 865) 256–257. "The Parliament is of the idea that the ePrivacy Regulation should be a standalone instrument and contain its own provisions, not depending on the Electronic Communications Code. Therefore, the Parliament suggests that the definitions from the Code be incorporated in the Proposal, taking into account any adaptation needed".

activity"[874]. However, such an exception may lower the expectation of privacy of end-users as metadata analysis – even if the information at stake might be regarded as *purely* technical – can provide insights on terminals' states which, in turn, may lead to draw inferences on end-users' habits. Traffic data (i.e., metadata) generated, processed and shared by IoT devices through electronic communications networks and services, increasingly "involve personal data processing"[875]. Section 4.3 will further address the risks of metadata analysis from a technical and legal integrated perspective.

Finally, as regards the relationship between the GDPR and the ePrivacy laws, Article 95 and recital 173 GDPR set the indisputable[876] *lex generalis* role of GDPR in EU data protection law. The ePrivacy Directive before, and possibly the Regulation afterwards, are *lex specialis* to the GDPR as they complement it with regard to the sector of electronic communications, insofar as those data processing operations involve personal data[877]. In this respect, the EDPB explains that the aim of Art. 95 GDPR is "to avoid the imposition of unnecessary administrative burdens upon controllers who would otherwise be subject to similar but not quite identical administrative burdens"[878].

4.1.1 Lawfulness: the challenges of 'consent' in IoT systems

Article 6(1) GDPR lays down the various legal grounds required by every processing involving personal data. At the same time, it substantiates the principle of 'lawful processing', enshrined in Art. 5 GDPR, and the provisions set forth by Art. 52(1) Charter of Fundamental Rights of the European Union ('CFR') and Art. 8(2) European Convention of Human Rights ('ECHR') establishing the conditions under which fundamental rights may be limited. "The function of Article 6(1) GDPR, seen in relation to Article 52(1) CFR, is to specify in more detail what the terms 'objectives of general interest (recognised by the Union)' and 'necessity to protect the rights and freedoms of others' mean in the context of data protection"[879].

Among the six grounds laid down by Art. 6(1) for making the processing of personal data lawful, for which the GDPR does not set any ranking, consent usually has a role "as a potential substitute

---

[874] Article 29 Data Protection Working Party, 'Opinion 01/2017 on the Proposed Regulation for the EPrivacy Regulation (2002/58/EC)' (2017) 28.

[875] EDPB, 'Opinion 5/2019 on the Interplay between the EPrivacy Directive and the GDPR, in Particular Regarding the Competence , Tasks and Powers of Data Protection Authorities' (2019) 12.

[876] *Contra* see Frederik Zuiderveen Borgesius, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) 5 International Data Privacy Law 163.

[877] The CJEU has endorsed this broad understanding of the concept of personal data: it is not necessary that all the information allowing the identification of the individual must be in possession of one person (see Judgment of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, paragraph 43).

[878] EDPB (n 875) 15.

[879] Waltraut Kotschy, 'Article 6 Lawfulness of Processing' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press 2020) 326.

whenever there is no contractual context, no detailed legal rules about a fitting legal basis or the scope of 'legitimate interests of the controller or of a third party' is particularly difficult to assess"[880]. For this reason, this sub-section dwells on the challenges that IoT systems pose to the notion of consent in EU privacy and data protection law.

Article 6(1)(a) GDPR provides for the lawfulness of the processing of personal data if the consent given by the data subject satisfies the conditions for valid consent in Art. 4(11), 7 and 8 GDPR. Consent must be freely given, specific, informed and unambiguous[881]. The cumulative nature of these criteria sets a high threshold to be met by data controllers[882]. In particular, Art. 7 GDPR, hinging on individual autonomy "as expressed via the right to informational self-determination"[883], lays down the conditions regarding the exercising of valid consent[884]. In line with the principle of accountability set forth in Art. 5 GDPR, the responsibility to prove that valid consent — pursuant to the conditions laid down in Art. 7 — was obtained from the data subject for a specific processing operation rest with the controller.

Importantly, Art. 7(3) mandates that controllers inform the data subject of the right to withdraw their consent at any time, before the consent is provided. Moreover, the consent shall be as easy to withdraw as to provide. "Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort"[885].

---

[880] ibid 329.

[881] Art. 4(11) GDPR.

[882] Lee A Bygrave and Luca Tosoni, 'Article 4(11). Consent' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press 2020) 181.

[883] Eleni Kosta, *Consent in European Data Protection Law*, vol 3 (Fabian Amtenbrink and Ramses A Wessel eds, Martinus Nijhoff Publishers 2013) 385.

[884] Eleni Kosta, 'Article 7 Conditions for Consent' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 350; the seminal Case C-673/17 *Planet 49 Gmbh v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* [2019] ECLI:EU:C:2019:801, and the Opinion delivered by the Advocate General Szpunar (ECLI:EU:C:2019:246). In particular, CJEU case *Planet49* may provide useful guidance vis-à-vis the interpretation of Article 7(4) as it concerns the assessment of whether consent may be *freely given* by means of 'pre-ticked' boxes. Moreover, the seminal case tackles the common practice of *bundling* consent to the processing of personal data to the provision of a service as part of a contract *even if the consent* (to the processing of personal data) *is not necessary for such execution*. Whereas Recital 43 GDPR suggests that such practices lead to a presumption that consent is not freely given, AG Szpunar interprets EU data protection law as meaning that "the prohibition on bundling is not absolute in nature" (para. 98). In the decision at issue, the AG concluded that consent to the processing of personal data is necessary for the conclusion of the contract i.e., participation in a prize game (para. 99). Despite this, the overturning of the presumption is "highly exceptional", see Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (2018) 9.

[885] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 884) 21.

Unsurprisingly, consent plays a prominent role in the ePrivacy Directive in relation to the confidentiality of communications. Thus, consent of the user or the subscriber is mentioned several times (e.g., Art. 5(3), 6, 9 and 13 ePD) as the only ground for the processing of their personal data. On the one hand, "the challenges that arise from the advancement of digital technologies, which the ePrivacy Directive aimed to tackle, justified the increased control of the user over the processing of his personal information and the protection of his privacy"[886]. On the other hand, the role of consent in the ePrivacy Directive has created numerous conceptual and application difficulties, in particular, having regard to the provision of consent for the storing of and access to the information already stored in the terminal equipment of the user, namely 'cookies' (Art. 5(3) ePD)[887].

The e-Privacy Directive defines consent, in Art. 2(f), by reference to the consent's definition enshrined in the Data Protection Directive, which has been repealed by Regulation (EU) 2016/679, that is, the GDPR. Therefore, this provision shall be read in conjunction with Art. 94 GDPR which stipulates that any reference to the repealed DPD shall be construed as references to the GDPR[888], while Art. 95 GDPR prohibits the imposition of additional obligations in relation to processing governed by the EPD. The Article 29 Working Party and several commentators evaluate this set of norms as to conclude that "the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e- Privacy Directive"[889].

However, according to Kosta, although the notion of consent should be understood in light of Article 4(11) GDPR, the specific requirements introduced in Article 7 GDPR should not apply in the electronic communications sector as they would create additional obligations, which would contradict the letter of Art. 95 GDPR. As a result, the reading of the two above-mentioned articles of the GDPR put the electronic communications operators in a quandary as to what standard to follow[890]. In 2019, the European Data Protection Board published an Opinion to clarify the interplay between the GDPR and the ePrivacy Directive where the processing triggers the material scope of both the legal instruments[891].

---

[886] Kosta, *Consent in European Data Protection Law* (n 883) 390.

[887] ibid 382–383. Art. 5(3) of the ePD, as modified by Directive 2009/136/EC, reads: "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service".

[888] Art. 94 GDPR.

[889] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 884) 4; Bygrave and Tosoni (n 882) 178.

[890] Kosta, 'Article 7 Conditions for Consent' (n 884) 348.

[891] EDPB (n 875).

In the Explanatory Memorandum to the Commission's Proposal for an ePrivacy Regulation, it is explicitly acknowledged that the "consent rule to protect the confidentiality of terminal equipment failed to reach its objectives as end-users face requests to accept tracking cookies without understanding their meaning and, in some cases, are even exposed to cookies being set without their consent"[892]. Art. 9 of the Commission's Proposal is exclusively dedicated to 'consent' as the pivoting lawful grounds for the processing of electronic communications data. In particular, Art. 9(1) clarifies that not only the definition of but also the conditions for consent provided for under Art. 4(11) and 7 GDPR respectively apply[893]. This provision would thus resolve the conflict highlighted by Kosta.

Possibly the biggest point of contention in the trialogue negotiations between the European co-legislators pivots around the broadening of the legal basis for the processing of electronic communications data so to include legitimate interest. Under the Croatian Presidency, the Council adopted a draft resolution that introduced the legitimate interest pursued by an electronic communications service or network provider and by a service provider as lawful grounds for the processing of electronic communication *metadata* (Art. 6b(1)(e); Recitals 17b and 17c) and to *use processing and storage capabilities of terminal equipment* or to *collect information* from an end-user's terminal equipment (Art. 8(1)(g); Recitals 21b and 21c) respectively. Eventually, the Council Proposal adopted in January 2021 under the German Presidency deleted those references, in line with the Opinion of the Article 29 Working Party[894].

To tackle some of the inherent challenges stemming from the overvaluation of consent with regard to the use of information stored in and related to end-users' terminal equipment (including IoT devices), the EDPB suggested that the new Art. 4a of the Council Proposal on consent (former Art. 9 of the Commission Proposal) should "go further and oblige browsers and operating systems to put in place a user friendly and effective mechanism allowing controllers to obtain consent, in order to create a level playing field between all actors[.] Privacy settings should preserve the right to the protection of personal data and the integrity of terminals of users by default and should facilitate expressing and withdrawing consent in an easy, binding and enforceable manner against all parties"[895]. In this respect, Articles 9(2) and 10 of the Parliament draft seem to offer a higher threshold of protection, in line with the conclusions of the EDPB: the technical settings of a software placed on the market permitting electronic communications, through which the user may consent to the use of processing and storage

[892] European Commission, 'Explanatory Memorandum of the Proposal for the ePrivacy Regulation' (n 16) 5.

[893] The Parliament draft version of the ePrivacy Regulation would remove the explicit reference to Articles 4(11) and 7 of the GDPR from the wording of Art. 9(1) ePR.

[894] Article 29 Data Protection Working Party, 'Opinion 01/2017 on the Proposed Regulation for the EPrivacy Regulation (2002/58/EC)' (n 874) 7.

[895] EDPB, 'Statement 03/2021 on the EPrivacy Regulation' (2021) 3.

capabilities, as well as the collection of information from end-users' terminal equipment (Art. 8(1)(b)), shall be binding for, and enforceable against any other party[896]. In this respect, the software's settings shall provide by design the option to prevent other parties from making use of the information under scrutiny and shall offer the option to opt out from cross-device tracking[897]. Moreover, the privacy settings shall be presented as to allow the end-user to take a fully informed decision and shall be easily accessible and modifiable during the use of the terminal equipment or software[898].

However, the fast-evolving electronic communications sector and the increasing pervasiveness of online environments led to both an *under* and *over*-valuation of consent, as stressed by Kosta. On the one hand, "the lack of direct communication [between the data subject and the data controller] renders it even more difficult to ensure that the data subject has been duly informed before the provision of his consent and the provided consent is freely given, uninfluenced from any negative forces. The reliance on privacy policies in online transactions that are often used for construing the consent of the users is questionable. The example of privacy policies illustrates that the mere reliance on consent often constitutes *under*-valuation of consent. The safeguarding of the privacy of the individuals should be complemented by a balance and proportionality test between the legitimate interest of the data controller that he wishes to serve via the obtaining of the user consent on the one hand and the privacy of the users on the other"[899].

On the other hand, "Art. 5(3) of the ePrivacy Directive seems to imply that the average user is able to understand the threats that are posed to his privacy by the installation and use of cookies and similar techniques and is able to make informed decisions on how to address them. However, the choice of the ePrivacy Directive to rely only on the consent of the data subject can be seen as an *over*-valuation of consent. The sole reliance on consent does not safeguard the protection of the privacy of the individual and should not be treated in itself as sufficient to legitimise all actions that infringe it. It should be complemented by a strict proportionality test in order to define the extent to which the providers can install cookies and collect information via them"[900]. In this respect, consent appears in practice as the 'silver bullet' to *lawfully* circumvent otherwise illegitimate data processing[901].

---

[896] Art. 9(2) Parliament ePrivacy Proposal.

[897] Art. 10(1) Parliament ePrivacy Proposal.

[898] Art. 10(2) Parliament ePrivacy Proposal.

[899] Kosta, *Consent in European Data Protection Law* (n 883) 391.

[900] ibid 393.

[901] Asia J Biega and Michèle Finck, 'Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems' [2021] Technology and Regulation 44, 52 <https://doi.org/10.26116/techreg.2021.004> accessed 3 May 2022; Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge University Press 2021) 52.

The above is all the more true in the field of IoT devices, where several legal expert commentators have already shed light on the *low-quality consent* that characterises the interaction between the users and their devices[902]. The typical hurdles of clicking/swiping and reading verbose and barely comprehensible privacy policies asking for consent are exacerbated by the inherent architectural complexity of IoT devices, bundling together almost invisible and always 'awake' sensors, actuators and networks (see Chapter 1). "Even where formally having been given some form of a 'notice' and opportunity to 'consent' to general terms and conditions, individuals often find themselves inside a system designed to maximise the monetisation of personal data, which leaves no real choice or control to individuals"[903]. Following this line of reasoning, Noto La Diega eventually comes to the conclusion that "consent can hardly be regarded as informed in most IoT scenarios, where users are unlikely to be aware of their Things' processing activities […] This is also due to the fact that Things are ubiquitous and tend to disappear, while the relational black box makes it arduous to map the players involved in the data flows"[904].

To overcome or, at least, mitigate these deficiencies, organisational and technological tools may be designed to uphold individual privacy and data protection (e.g., Privacy Enhancing Technologies, PETs)[905]. As regards the former, many IoT resource-constrained devices present small screens, or none at all, with limited room for information: "a layered way of presenting information can be considered, where appropriate, to avoid excessive disturbance of user experience or product design"[906]. In terms of technological solutions, Koolen, among others, suggests a 'consent management platform' that would streamline the consent process in a IoT environment: "a dedicated software tool or an online page could be created where consumers can keep track of all smart devices that are present in their household, see information regarding privacy settings, and modify their consent vis-à-vis the collection of certain categories of personal data. It is imperative that such a digitally designed environment allows for ease of use"[907]. The reading of the Parliament draft of the

---

[902] Pagallo, Durante and Monteleone (n 77) 64; Christof Koolen, 'Transparency and Consent in Data-Driven Smart Environments' (2021) 7 European Data Protection Law Review 174, 185.

[903] EDPS, 'Opinion 9/2016 EDPS Opinion on Personal Information Management Systems: Towards More User Empowerment in Managing and Processing Personal Data' (2016) 5 <https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en>.

[904] Guido Noto La Diega, *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies* (Routledge, Taylor and Francis Inc 2023) 242.

[905] ENISA, 'A Tool on Privacy Enhancing Technologies (PETs) Knowledge Management and Maturity Assessment' (2017); Lee A Bygrave and Dag Wiese Schartum, 'Consent, Proportionality and Collective Power', *Reinventing Data Protection?* (Springer Netherlands 2009); European Commission, 'Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) COM(2007) 228 Final' (2007) <http://eurlex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf> accessed 9 May 2022.

[906] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 884) 14.

[907] Koolen (n 902) 186.

ePrivacy Regulation, in particular, having regard to Article 8, 9 and 10, in conjunction with the Statement of the EDPB, would indeed require the development of such solutions.

However, even if the data subject does not consent to some specific processing, the real lack of control over one's own information brought about by the IoT era precisely lies in those undertakings that are often still able to draw probabilistic inferences from other data collected from that same individual[908]. This, in turn, brings us to the next legal challenge involving one core principle of EU data protection, that is, transparency. The obligation to provide the information related to the personal data processing in a transparent fashion is linked to consent in that there must always be information before there can be consent[909]. It is no coincidence that transparency mechanisms or tools (such as privacy icons) are often presented to substantiate the requirement of 'informed consent'[910].

4.1.2 Lack of control and information asymmetry: IoT and transparency

Before engaging in the discussion on transparency in IoT from a European privacy and data protection perspective, a terminological point must be made. The title used for the present section, i.e. 'lack of control and information asymmetry' hinges on the first legal challenge identified by the Article 29 Working Party in the above-mentioned Opinion on the IoT. The Working Party puts forward the issue of users' control over their own data in terms of whether or not the collection and processing of their data has been made in a *transparent* manner or not[911].

This, in turn, reflects systemic information asymmetry between users and IoT stakeholders (e.g., device manufacturers, APIs developers, generic third parties, and IoT data platforms, regardless of whether they qualify as data controllers)[912], as the former are often unaware of what data, for what purpose(s), and for how long is extracted by the latter: "in the absence of the possibility to effectively control how objects interact or to be able to define virtual boundaries by defining active or non-active zones for specific things, it will become extraordinarily difficult to control the generated flow of data"[913]. Even though transparency is an essential feature of ownership, this section avoids questions

---

[908] ibid 185.

[909] Opinion of Advocate General Szpunar in Case C-673/ 17, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.,* delivered on 21 March 2019, ECLI:EU:C:2019:246, para. 112.

[910] Aurelia Tamò-Larrieux, *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things* (Springer 2018) 155.

[911] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 851) 6.

[912] Tamò-Larrieux (n 910) 63.

[913] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 851) 6.

regarding the ownership of data generated by IoT devices[914], debates on data ownership in the EU[915] and power asymmetries between data subjects and corporate data users[916].

Moreover, against the background of market and information asymmetries between IoT manufacturers and IoT users, in 2022 the Commission proposed the so-called Data Act[917], yet another pillar of the EU strategy for data (February 2020), which integrates the Data Governance Act[918]. The Data Act aims *inter alia* to give users access to data generated by them, which is often exclusively harvested by manufacturers; and to share such data with third parties to provide aftermarket or other data-driven innovative services. Even though the Data Act falls outside the scope of this investigation, it is worth mentioning that the Proposal's goal of unleashing the potential of information to be extracted from IoT data needs to be streamlined with the EU *acquis* in the field of personal data protection[919].

'Lack of control and information asymmetry' might also implicate a wide debate on the notion of *group privacy* and *collective data protection*[920]. Although not the subject of this Chapter, as the personal data processing in IoT systems increasingly 'belongs to' clusters of individuals, this topic looms in the background. "Individuals are more often targeted as a member of a group, whereas they can even ignore being a part of that group on the basis of a set of ontological and epistemological

---

[914] Noto La Diega (n 904) 68–115. See also Václav Janeček, 'Ownership of Personal Data in the Internet of Things' (2018) 34 Computer Law & Security Review 1039; Thomas J Farkas, 'Data Created by the Internet of Things: The New Gold without Ownership?' (2017) 23 Revista La Propiedad Inmaterial 5; Alberto De Franceschi and Michael Lehmann, 'Data as Tradeable Commodity and New Measures for Their Protection' (2015) 1 The Italian Law Journal 51; Sjaak Wolfert and others, 'Big Data in Smart Farming – A Review' (2017) 153 Agricultural Systems 69; Josef Drexl, 'Designing Competitive Markets for Industrial Data - Between Propertisation and Access' (2017) 8 JIPITEC 257.

[915] Gianclaudio Malgieri, 'Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data ' (2016) 4 Privacy in Germany 133; Nadezhda Purtova, *Property Rights in Personal Data: A European Perspective* (Wolters Kluwer Law International 2012); Nadezhda Purtova, 'Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatization, and Ambient Intelligence' in Serge Gutwirth and others (eds), *Computers, Privacy and Data Protection: An Element of Choice* (Springer 2011); Sjef Van Erp, 'Ownership of Data: The Numerus Clausus of Legal Objects' (2017) 6 Property Rights Conference Journal 235.

[916] Barbara Prainsack, 'Logged out: Ownership, Exclusion and Public Value in the Digital Data and Information Commons' (2019) 6 Big Data & Society.

[917] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final (23.2.2022).

[918] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[919] EDPB - EDPS, 'EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (2022) <https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf>; Inge Graef and Martin Husovec, 'Seven Things to Improve in the Data Act' [2022] SSRN Electronic Journal. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793>; Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act Will Not Fulfill Its Objectives' [2022] SSRN Electronic Journal <https://papers.ssrn.com/abstract=4080436> accessed 12 July 2022.

[920] Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy* (Springer 2017); Pagallo, 'The Group, the Private, and the Individual: A New Level of Data Protection?' (n 203).

predicates that cluster people into multiple categories"[921]. This leaves many issues open: how should we grasp the definition of group? What kind of right should the law grant a group? Pagallo et al. elaborate on the ECtHR seminal case in EU data retention field *Big Brother Watch and others v. UK* (further addressed in section 4.3) to assert the existence in EU law of "a procedural right to a judicial remedy against governments and states in the sphere of private life, i.e. on the basis of personal damage suffered by some individuals, such as the applicants and members of the group"[922]. According to the authors, this view is reflected in the rationale underpinning Articles 80(1) and 80(2) GDPR: "[S]ince the data subject can be targeted and her privacy infringed due to her membership in a given (racial, ethnic, genetic, etc.) data group, it makes sense to grant such a group, or "anybody, organisation or association which aims to protect data subjects' rights and interests," a procedural right to a judicial remedy against the data controllers, processors or supervisory authorities"[923].

European legal systems traditionally address, by proxy, data protection as *transparency*, whereas privacy is generally understood as a 'tool for *opacity*'[924]. The transparency principle is explained in Recital 39 GDPR[925] and Recital 58 further illustrates its scope and relevance vis-à-vis increasing digitisation, where the IoT is only one element of a more complex picture. On the one hand, *transparency* "requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used"[926]. On the other hand, the Regulation acknowledges that "the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising"[927]. Furthermore, in a specific context of advertising, that is, real-time bidding (RTB), some authors argue that core GDPR

---

[921] Pagallo, Durante and Monteleone (n 77) 67.

[922] ibid 69.

[923] ibid 70.

[924] Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006) 62; Pagallo, Durante and Monteleone (n 77) 62.

[925] Recital 39 GDPR: "It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used".

[926] Recital 58 GDPR.

[927] ibid.

requirements including *inter alia* the transparency principle and informed consent are irreconcilable with the fundamental functioning of RTBs[928].

Article 5(1)(a) GDPR states that personal data must be processed in a transparent manner in relation to the data subject, while Art. 12(1) mandates that the data controller has to take appropriate measures to provide any information to the data subject, either whether personal data are collected from the data subject or have not been obtained from him/her (Articles 13 and 14 GDPR respectively)[929], and any communication under Articles 15 to 22 and 34 relating to processing *in a concise, transparent, intelligible and easily accessible form, using clear and plain language*, in particular for any information addressed specifically to a child.

In that respect, the rationale of Art. 12 is to provide for procedural provisions – and not substantive rights – to inform and regulate the information flow between controllers and data subjects as regards the underlying personal data processing: data subjects' substantive rights, notably the right of access to personal data[930], "can serve their purpose only if supported by clear, proportionate and effective procedures"[931].

As also mentioned earlier, the ePrivacy Directive applies to IoT devices insofar as they qualify as 'terminal equipment'[932]. Albeit the principle of transparency is not explicitly posited by the Directive as in the GDPR, Articles 5(3), 6(4) and 9 ePD add important provisions in terms of transparency – which is linked to consent – obligations of undertakings in the field of internet-connected devices.

In particular, Art. 5(3) mandates that in order to store or access information already stored in users' terminal equipment, providers must give users clear and comprehensive information about the

---

[928] Michael Veale, Midas Nouwens and Cristiana Teixeira Santos, 'Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?' (2022) 2022 Technology and Regulation 12, 19.

[929] Cécile De Terwangne, 'Article 5. Principle Relating to Processing of Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 315: the author notes that certain aspects of Articles 12-14 are more connected to the fariness requirement.

[930] European courts have ruled on information and access rights in multiple cases. As regards the CJEU, see *inter alia* Case C-131/12, *Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317; Joined Cases C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* [2014] ECLI:EU:C:2014:2081; Case C-486/ 12, *X* [2013] ECLI:EU:C:2013:836. As regards the ECtHR, it should be noted that the ECHR lacks a provision that define and regulates the exercise of access and information rights. However, the Court consistently implies that information and access rights are core components of Art. 8 ECHR and other fundamental rights. See, *ex multis*, ECtHR, 18 May 2010, (Application no 26839/ 05) *Kennedy v United Kingdom*; ECtHR, 25 September 2012, (Application no. 33783/ 09), *Godelli v Italy*; ECtHR, 4 December 2015, (Application no. 47143/ 06), *Roman Zakharov v Russia*.

[931] Radim Polčák, 'Article 12. Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subject' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 401.

[932] Koolen (n 902) 178.

purposes of the processing. Such disclosure is prodromal to consent[933]. Moreover, as regards the processing of metadata, Articles 6(4) and 9(1) ePD stipulate that providers must inform the users of the types of *traffic* and *location data* that are processed, of the duration of such processing and whether the (location) data will be transmitted to a third party, prior to obtaining the consent of users or subscribers.

When it comes to the Proposal for an ePrivacy Regulation, Art. 8 – dealing with the protection of information stored in and related to end-users' terminal equipment –paragraph 2, letter b, mandates that "a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection"[934]. Importantly, the information may be provided through *standardised icons* to give a meaningful account of the processing in a "easily visible, intelligible and clearly legible manner"[935].

As regards the processing of electronic communications data, i.e. coupling together content and metadata, the Commission's Proposal does not explicitly lay down a transparency obligation: as seen in the previous section, providers of electronic communications services may process metadata, among the various legal grounds, if the end-users concerned have given their *consent* to the processing of their communications metadata for *one or more specified purposes*, provided that the purposes under scrutiny could not be achieved through anonymisation techniques[936]. Conversely, a transparency requirement can be tracked having regard to the information that undertakings shall provide to end-users for privacy settings and options: the software has to inform end-users about the privacy settings options and require the end-users' consent to a setting afterwards[937].

Despite the existence of these instruments – while awaiting the ePrivacy Regulation, IoT environments make a fully-fledged application of the principle of transparency rather challenging due to i) architectural constraints; ii) multiple and hardly traceable data flows; iii) multiple actors involved in the processing.

To overcome these challenges, legal and technical literature have proposed to employ 'transparency tools'. These solutions typically combine technical measures with design features. Article 12(7)

---

[933] Art. 5(3) ePD: "[…] the subscriber or user concerned has given his or her consent, *having been provided* with clear and comprehensive information".

[934] Art. 8(2)(b) ePrivacy Regulation Proposal; recital 20 ePrivacy Regulation. This provision will be further addressed in section 4.3.2 with regard to a possible lowering of the level of protection accorded by the GDPR.

[935] Art. 8(3) ePrivacy Regulation Proposal.

[936] Art. 6(2)(c) ePrivacy Regulation Proposal.

[937] Art. 10(2) ePrivacy Regulation Proposal.

GDPR and Article 8(3) of the Commission's ePrivacy Regulation Proposal set forth a possibility for data controllers and service providers respectively to comply with their obligation to inform data subjects *via* 'standardised icons' that should help (and empower) the data subject in visualising the privacy setting from the outset of the data processing life cycle. Icons, however, are just one of the "multiple additional options for how a controller can inform data subjects besides textual or spoken form. Thus, a controller can also use pictures or other forms of expression that are not standardised icons under Article 12(7) GDPR if these alternative means of expression provide for 'concise, transparent, intelligible and easily accessible' information"[938].

Thus, privacy certificates or labels (similarly to cybersecurity labels, see Section 3.3.2) address the need to verify that data controllers' processing operations comply with the relevant legal standards[939]. "Once verified, a product or service provider can post the certificate icon in order to publicly indicate that the company adheres to the standards of the certification authority"[940].

Push notifications are yet another fitting example suggested by scholars to present information in a clear and short fashion[941]. "If a consumer issued a voice command to his smart speaker, a notification could show up on his phone immediately afterwards, reminding the user of the voice analysis process that takes place in the background"[942].

Against this backdrop, it should be investigated whether existing IoT architectures provide technological solutions in terms of transparency. In 2018, Janeček answered negatively[943]. Without dwelling on empirical research over existing market solutions too extensively, three case-studies from industry-leading companies can nonetheless be considered.

Apple Inc. deployed important privacy features intended to help users make more informed decisions about their personal data. In particular, through a feature called the 'Privacy Nutrition Label', Apple requires every app — including its own — to provide users with a standardised, easy-to-view

---

[938] Polčák (n 931) 410.

[939] Alexandr Railean and Delphine Reinhardt, 'Let There Be Lite: Design and Evaluation of a Label for IoT Transparency Enhancement', *MobileHCI 2018 - Beyond Mobile: The Next 20 Years - 20th International Conference on Human-Computer Interaction with Mobile Devices and Services, Conference Proceedings Adjunct* (2018); Alexandr Railean and Delphine Reinhardt, 'OnLITE: On-Line Label for IoT Transparency Enhancement' in Mikael Asplund and Simin Nadjm-Tehrani (eds), *Secure IT Systems - 25th Nordic Conference (NordSec 2020)* (Springer International Publishing 2021); Rob van Diermen, 'The Internet of Things: A Privacy Label for IoT Products in a Consumer Market' (University of Leiden 2018) <https://openaccess.leidenuniv.nl/handle/1887/64571>; Yun Shen and Pierre Antoine Vervier, 'IoT Security and Privacy Labels' in Maurizio Naldi and others (eds), *Privacy Technologies and Policy, 7th Annual Privacy Forum* (Springer, Cham 2019).

[940] Tamò-Larrieux (n 910) 137.

[941] Gilad Rosner and Erin Kenneally, 'Privacy and the Internet of Things: Emerging Frameworks for Policy and Design', *Berkeley Center for Long-Term Cybersecurity (CLTC) White Paper Series* (2018) 16–19.

[942] Koolen (n 902) 182.

[943] Janeček (n 914) 1046.

overview of the developer's data processing practices. The label give users key information about how an app uses their data — including whether the data is used to track them, linked to them, or not linked to them. Moreover, another feature, namely the 'App Tracking Transparency', "will require apps to get the user's permission before tracking their data across apps or websites owned by other companies. Under 'Settings', users will be able to see which apps have requested permission to track and make changes as they see fit"[944].

In 2021, Samsung also highlighted its commitment towards transparency in the context of smart devices' data processing. "Consumers, developers and partners are given the information needed to make decisions about how data is managed. The company offers users the option to review and manage their permissions from privacy setting on their Galaxy devices and Smart TVs and discloses Samsung's privacy policies through the Privacy Portal. Going forward, Samsung will collaborate with global security experts while continuing to release open-source security analysis tools to make its ecosystems more secure"[945].

Lastly, Xiaomi published an 'IoT users' privacy white paper', with the aim of casting light on the data protection practices of the company. In the white paper, Xiaomi breaks down data collections details and specific privacy & data protection features for six IoT products and three associated mobile applications with a view to enabling customers to develop a full understanding of how the company collect, use, and store data[946].

In conclusion, transparency enhancing tools (TETs), deploying models such as 'privacy information management systems' (PIMS) or 'personal data management systems' (PDMS), may help in rebalancing the information asymmetry between consumers (i.e., data subjects) and digital market companies by providing the former with actual means to deal with the processing of their personal data and, therefore, to fully exercise the rights granted by the GDPR[947]. As stated in the previous section, technical solutions such as user-friendly dashboards, which would display the information relevant to the data processing in a layered structure, also through the adoption of push notifications, would help to overcome inherent hurdles of the IoT ecosystem. These technical solutions would benefit both data subjects and digital providers. Awareness over complex data processing, including

---

[944] Apple, 'Data Privacy Day at Apple: Improving transparency and empowering users' (2021) Press release, available at < https://www.apple.com/hk/en/newsroom/2021/01/data-privacy-day-at-apple-improving-transparency-and-empowering-users/> accessed 21 April 2022.

[945] Samsung, 'Samsung Unveils Solutions for a New Era of Connected Experiences at SDC 21' (2021) Press release <https://news.samsung.com/us/samsung-sdc-2021-solutions-connected-experiences/> accessed 20 April 2022.

[946] Xiaomi, 'Xiaomi IoT Privacy White Paper' (2021) <https://trust.mi.com/> accessed 21 April 2022.

[947] Alessandro Bernes, 'Enhancing Transparency of Data Processing and Data Subject's Rights Through Technical Tools: The PIMS and PDS Solution' in Roberto Senigaglia, Claudia Irti and Alessandro Bernes (eds), *Privacy and Data Protection in Software Services* (Springer Nature 2022) 200.

storage, transmission and profiling will be enhanced and users, from being passive subjects in the 'data economy', will undertake a more proactive role whereas market players will interact better with their customers, and enjoy a more solid compliance with the EU data protection legal framework (in particular, regarding the accountability principle and Data Protection by Design)[948].

4.1.3 Lack of adequate security controls: eschewing the scenario of an 'Internet of *un*secure Things'

The last legal challenge identified by the Article 29 Working Party hinges on the upward trend of information and network security risks raised, in particular, by resource-constrained devices. Section 1.3 of the first Chapter already pointed out that many resource-constrained IoT devices may not have the computational power to run encryption algorithms. The Working Party explicitly states that "most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries"[949]. There is an urgent need therefore to develop security, privacy and data protection technical solutions for data at rest or in transit in constrained connected environments as well as secure mechanisms for horizontal handover[950]. In this respect, Chapter 1, section 3 already shed light on the present discussion surrounding lightweight cryptographic standards and protocols for IoT resource-constrained devices[951].

Art. 32 GDPR mandates that controllers and processors implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals. Importantly, encryption is explicitly listed in Art. 32 GDPR as a security (technical) measure that controllers and processors should implement 'as appropriate'[952].

Albeit the deployment of encryption protocols is not *per se* mandatory, "Article 32 express a clear preference for them, making it likely that regulators will expect data controllers and processors to use

---

[948] ibid 200–201.

[949] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 851) 9.

[950] ENISA, 'Ad-Hoc & Sensor Networking for M2M Communications Threat Landscape and Good Practice Guide', vol 83 (2017) 66 <https://www.enisa.europa.eu/publications/m2m-communications-threat-landscape>; Scott J Shackelford, *The Internet of Things, What Everyone Needs to Know* (Oxford University Press 2020) 71–72.

[951] Sherali Zeadally, Ashok Kumar Das and Nicolas Sklavos, 'Cryptographic Technologies and Protocol Standards for Internet of Things' (2021) 14 Internet of Things 6–7; Syed Rizvi and others, 'Threat Model for Securing Internet of Things (IoT) Network at Device-Level' (2020) 11 Internet of Things 100240.

[952] Tamò-Larrieux (n 61) 170: "Art. 32 relies on common terms from computer science, such as confidentiality, integrity, and availability, with which developers are familiar. Additionally, it broadens the scope of "security" by elaborating on pseudonymization or restoring availability and access after an incident. It thus provides broader guidance to data controllers while remaining technology- neutral".

them whenever possible"[953]. In this respect, the CJEU is expected to answer the questions referred in a request for a preliminary ruling in the Case C-340/21[954] on the interpretation of *inter alia* Art. 32. In particular, the Court is asked to cast light on what the subject matter and scope of the judicial review of legality in the examination should be as to whether the technical and organisational measures implemented by the controller are appropriate pursuant to Article 32 of Regulation (EU) 2016/679.

Whereas the ePrivacy Directive contains a specific provision on the 'security of processing' – as amended by Directive 2009/136/EC, the ePrivacy Regulation Proposal does not specifically address matters concerning the processing of personal data in order to ensure alignment with the GDPR which – as already mentioned – would be applicable as *lex generalis*[955]. Thus, the revision of the ePD of 2009 added several paragraphs to Art. 4 specifying, on the one hand, the objectives of the (security) technical measures[956] and, on the other hand, notification duties for the provider of publicly available electronic communications services in the case of personal data breaches. With a view to eliminating regulatory duplication, which inevitably leads to confusion, the proposed Regulation repeals ePD security rules on the processing of data. In particular, the Proposal makes reference to Article 32 GDPR with regard to the protection of information stored in and related to end-users' terminal equipment[957].

Conversely, the ePrivacy Regulation would relate to (network) security risks and provides for an obligation upon providers of electronic communications services to alert end-users in the event of a particular risk that may compromise the security of networks and services. In the Commission Proposal, Art. 17 postulates that providers of electronic communications services shall inform end-users of risks that may compromise the security of networks and underlying services. If the risk cannot be mitigated by the measures to be taken by the provider, the latter shall inform end-users of any possible remedies.

Whilst the Council deletes this provision from the Commission's draft, Parliament amends it heavily. The first problematic aspect that needs to be considered is the likely overlap with the NISD and especially NIS2 notification duties (see Chapter 3.5), which may create duplicative requirements and

---

[953] Burton (n 237) 636.

[954] Request for a preliminary ruling from the *Varhoven administrativen sad* (Bulgaria) lodged on 2 June 2021 — *VB v Natsionalna agentsia za prihodite*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CN0340> accessed 10 April 2022.

[955] European Commission, 'Explanatory Memorandum of the Proposal for the ePrivacy Regulation' (2017) 2.

[956] Ensuring the authentication principle, protecting personal data stored or transmitted against accidental or unlawful destruction, loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure and ensuring the implementation of security policies.

[957] Art. 8(2) ePrivacy Regulation Proposal.

bring legal uncertainty. The Parliament's amendment specifying that Art. 17 ePR should be without prejudice to the obligations provided for in Directive (EU) 2016/1148 is too vague; the EU co-legislators should, in that regard, ensure effective alignment with the NIS2 relevant provisions to strengthen legal coherence between the Union acts of the Digital Single Market.

Furthermore, it is explicitly stressed that providers shall ensure the confidentiality, integrity and protection against unauthorised access to the electronic communications data, either in transmission or stored, by means of "cryptographic methods including end-to-end encryption of the electronic communications data. When encryption of electronic communications data is used, decryption by anybody else than the user shall be prohibited"[958].

Importantly, the Parliament also stresses that Member States shall refrain from the "weakening of the confidentiality and integrity of their networks and services or the terminal equipment, including the encryption methods used"[959] by imposing any obligations on either electronic communications service providers or software manufacturers. The stance adopted by the European Parliament against the weakening of cryptographic methods (e.g., end-to-end encryption), will be assessed against the background of the so-called 'crypto-wars' or 'encryption debate' which still animates the public debate[960]. Section 4.3 will shed further light on the policy debates surrounding encryption.

Moreover, Parliament would place a second negative obligation on providers of electronic communications services, providers of information society services, and manufacturers of software permitting the retrieval and presentation of information on the internet: these entities must refrain from preventing users and subscribers from applying the best available techniques against intrusions and interceptions and to secure their networks, terminal equipment and electronic communications[961].

All in all, it remains to be seen whether the Parliament's clear stand against the weakening of encryption has to prevail in the ePrivacy Regulation trilogue negotiations. The next section will therefore focus, from an interdisciplinary technical and legal standpoint, on cryptographic methods, including encryption which should be considered as an interface between 'security' and 'privacy'.

---

[958] Art. 17(1a) Parliament Proposal.

[959] *Ibid.*

[960] Koops and Kosta (n 137); Ziccardi, 'The GDPR and the LIBE Study on the Use of Hacking Tools by Law Enforcement Agencies' (n 137).

[961] Art. 17(1b) Parliament ePrivacy Proposal.

4.2 The Role of Encryption vis-à-vis the Fundamental Rights to Privacy and Data Protection

This section hinges on the relationship between various cryptographic technical tools, having regard, but not limited to, encryption, and the traditional legal disciplines of privacy and data protection. Thus, an alignment of privacy, data protection and *cybersecurity* – to be understood broadly to cover information security (see Chapter 2) – is particularly striking when it comes to cryptographic technologies that aim to ensure confidentiality in the processing process, in particular, regarding data sharing and network communication.

In order to assess the relationship between encryption and pseudonymisation, it is necessary to insist on an epistemological and technical inquiry about the foundations of the two data protection techniques primarily envisaged by Art. 32 GDPR. In section 4.2.1, the analysis sheds light on the rationale of encryption which substantially differs from hashing and pseudonymisation, albeit the latter is generally achieved by means of cryptography, and why this distinction matters when it comes to uphold the fundamental rights to privacy and data protection. Afterwards, the legal investigation casts light – in section 4.2.2 – on whether and to what extent state-of-the-art encryption protocols challenge the already blurred distinction between personal and non-personal data, underlying the EU data protection legal framework. Finally, in section 4.2.3 the discussion considers the often-overlooked impact of encryption on *privacy,* in terms of infringement of the fundamental right it aims to protect.

4.2.1 The quest for encryption, beyond pseudonymisation: a technical perspective

Since ancient times, society has felt the need to masquerade sensitive information: cryptography has always been a way to guarantee information security[962]. Back to the present day, our increasingly data-driven society has exacerbated this need[963]: Internet of Things (IoT) resource-constrained devices absolutely require encryption protocols suited to their storage and computational power capacities in order to secure data flow[964]. European privacy and data protection law, as already mentioned in section 4.1.3, primarily rely on encryption to ensure the fundamental rights to privacy and protection of personal data on the one hand, and on the other, the principles underpinning information security. Recently, the European Data Protection Supervisor claimed that encryption is "natural mean for data

[962] John F Dooley, *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms* (Springer 2018); Donald Davies, 'A Brief History of Cryptography' (1997) 2 Information Security Technical Report 14.

[963] Jose L Hernandez-Ramos and others, 'Toward a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data-Protection Policies' (2020) 18 IEEE Security and Privacy 28.

[964] Rayes and Salam (n 13) 211; Marwedel (n 16) 191–193; Serpanos and Wolf (n 315) 59–81; Pagallo, Durante and Monteleone (n 77).

protection, and for personal data protection as well: GDPR, in this sense, is reflecting a natural state"[965].

It is worth clarifying from the outset that the concept of 'encryption' may be misleading, or simplistically broad: without dwelling on the various cryptographic algorithms too extensively, a classification is needed. Amongst the various cryptographic tools, computer science literature historically makes a first distinction between symmetric and asymmetric encryption.

Symmetric or private-key cryptography came first. Using mathematical operations, this technique aims to hide the content, by rendering the information unintelligible to anyone who does not have the cryptographic key[966]. In this respect, it is a two-way function: what is encrypted, *via* an algorithm called a "cipher", can be decrypted with the proper key. The *plain text* becomes *cyphertext* after the mathematical process. As a result, without the cryptographic key, no one can theoretically see the content of the message i.e., the plain text. Block ciphers are the most widely spread symmetric encryption algorithms[967].

Building on symmetric-key techniques, cryptographic hash functions are mostly adopted in symmetric-key setting[968]. They are commonly referred to as one-way functions, i.e. an irreversible process aiming at scrambling variable-size plain text to produce a unique fixed-size message digest (i.e. the message output)[969]. The primary requirement is to be 'collision resistant', with a collision being two inputs that map to the same plain text. In recent years, the most widely used hash function has been the Secure Hash Algorithm (SHA), developed by the federal US Agency NIST.

The main difference between symmetric and asymmetric encryption is that the latter involves the use of two separate keys, whereas the former only adopts one key[970]. This approach predicates on the possibility of widely distributing one key, the public key, while the other, i.e. the secret key, must be

---

[965] Wojciech Wiewiórowski, 'Keynote: Data Protection Needs Encryption' *EDPS, 1st Online IPEN Workshop* (3 June 2020).

[966] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (Wiley Inc., 1995), 21.

[967] Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*, vol 6 (CRC Press Taylor & Francis Group 2015) 77; William Stallings and Lawrence Brown, *Computer Security: Principles and Practice* (4th edition, Pearson 2018) 55: A block cipher processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block. The algorithm processes longer plaintext amounts as a series of fixed-size blocks. The most important symmetric algorithms, all of which are block ciphers, are the Data Encryption Standard (DES), triple DES, and the Advanced Encryption Standard (AES)".

[968] Katz and Lindell (n 967) 153.

[969] EDPS and AEPD, *Introduction to the Hash Function as a Personal Data Pseudonymisation Technique* (2019), 8-10.

[970] Stallings and Brown (n 967) 67.

kept secured[971]. In the classical example, Alice wants to send a message to Bob. Alice encrypts a message with Bob's public key; Bob then uses his private key to decrypt the resulting ciphertext.

An advanced asymmetric cryptographic scheme is represented by *homomorphic encryption*, which has been referred to as the 'Swiss army knife' of cryptography due to its extreme versatility[972]. Broadly speaking, it refers to those schemes that perform computation on encrypted data. "Secure multiparty computation epitomises the promise of cryptography, performing the seemingly impossible magic trick of processing data without having access to it"[973]. "In addition to the usual encryption and decryption procedures, these schemes have an evaluation procedure that takes ciphertexts encrypting *x* and a description of a function *f*, and returns an "evaluated ciphertext" that can be decrypted to obtain the value *f(x)*"[974]. In terms of confidentiality properties, it is worth noting that the evaluated ciphertext does not reveal *f* even to the owner of the (secret) key. As addressed in the next section, homomorphic encryption may solve many open issues in terms of privacy preservation in IoT environments[975].

Pseudonymisation, instead, is conceived by the GDPR[976] as a means of *reducing* risks to data subjects[977] by hiding the identity of individuals in a dataset. More precisely, it hinges on the replacement of one or more personal data identifiers with so-called pseudonyms, provided that the link between the pseudonyms and the initial identifiers are *adequately* protected[978].

Hence, EU data protection legislation relies on pseudonymisation as a technical measure that can support data protection by design (Art. 25 GDPR) and the security of personal data processing (Art. 32 GDPR). Thus, pseudonymisation has been widely acknowledged as a 'privacy enhancing

---

[971] Richard R Brooks, *Introduction to Computer and Network Security: Navigating Shades of Gray* (1st Editio, Chapman and Hall/CRC Routledge 2014) 100.

[972] Boaz Barak and Zvika Brakerski, 'The Swiss Army Knife of Cryptography ' (*Windows on Theory - A Research Blog*, 2012) <https://windowsontheory.org/2012/05/01/the-swiss-army-knife-of-cryptography/> accessed 7 April 2022.

[973] Shai Halevi, 'Homomorphic Encryption' in Yehuda Lindell (ed), *Tutorials on the Foundations of Cryptography* (Springer International Publishing 2017) 219.

[974] ibid 220.

[975] ENISA, 'Data Protection Engineering: From Theory to Practice' (2022) 14; Christoph Heinz and others, 'Privacy, GDPR, and Homomorphic Encryption' in Carna Zivkovic, Yajuan Guan and Christoph Grimm (eds), *IoT Platforms, Use Cases, Privacy, and Business Models: With Hands-on Examples Based on the VICINITY Platform* (Springer Nature 2021) 176.

[976] Art. 4(5) GDPR: "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

[977] Recital 28 GDPR.

[978] ENISA, 'Recommendations on Shaping Technology According to GDPR Provisions: An Overview on Data Pseudonymisation' (2018).

technology'[979]: not only does it masquerade data subjects' identities, but it can also contribute towards the data protection principle of data minimisation and data accuracy as data controllers and/or processors process 'real' information (contrary to synthetic data) without having access to the identities of the data subjects to whom the information relates.

Even though the risk of (re)identification is reduced, pseudonymised data fall nevertheless within the scope of GDPR: it is certainly true that such processing prevents direct identification through attribution, but not through the test set by Recital 26 GDPR[980], which clearly specifies the personal nature of such data.

In 2019, ENISA dedicated a report to shed light on the 'basic' pseudonymisation techniques that are applied. These are: counter; random number generator (RNG); hash function; message authentication code (MAC); symmetric encryption[981]. A report from 2021 further discusses more advanced techniques that can provide more sophisticated pseudonymisation solutions in real world scenarios, such as asymmetric encryption and homomorphic encryption, secure multiparty computation, zero-knowledge proof, secret sharing schemes and chaining mode[982]. From the work of ENISA, a key takeaway is that a risk-based and case-by-case approach is needed with regard to the choice of the correct pseudonymisation technique to implement. The best possible technique should be selected to properly address and mitigate the relevant privacy threats for the scenario in question.

From the above, it follows that the relation link between pseudonymisation and encryption might be built upon a 'speciality criterion', based on the different scope and rationale. First, cryptographic techniques, such as encryption, are effectively used *as* pseudonymisation techniques, and not the other way round. In the same vein as ENISA, among the most used pseudonymisation techniques, the Article 29 Working Party listed symmetric encryption, such as block ciphers (AES algorithms), hash

[979] ENISA, 'Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics' (2015) <https://www.enisa.europa.eu/publications/big-data-protection> accessed 18 February 2020; ENISA, 'Data Protection Engineering: From Theory to Practice' (n 975).

[980] Miranda Mourby and others, 'Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK' (2018) 34 Computer Law and Security Review 222, 225.

[981] ENISA, 'Pseudonymisation Techniques and Best Practices: Recommendations on Shaping Technology According to Data Protection and Privacy Provisions' (2019) 21–26.

[982] ENISA, 'Data Pseudonymisation Techniques: Advanced Techniques & Use Cases. Technical Analysis of Cybersecurity Measures in Data Protection and Privacy' (2021) 14–26.

function (either with stored or deleted key) and so-called pepper[983] or salted hash[984]. Second, the rationale underpinning encryption is to potentially protect any kind and any size of data or information, resulting therefore in a broader scope than pseudonymisation. Thus, different encryption protocols follow the entire data flow to address either data at rest (storage encryption) or data in motion (transmission encryption)[985]. Conversely, the scope of pseudonymisation only considers the personal identifiers. Third, another variable of this analysis is predicated on the semantic value of the resulting text after these techniques have been implemented. Contrary to encrypted data, pseudonymised data still provide some legible information: a third party may still be able to understand the underlying structure of data[986]. Indeed, it is worth noting that the GDPR deems pseudonymisation an appropriate safeguard for any processing for scientific, historical or statistical purposes[987].

4.2.2 State-of-the-art encryption and pseudonymisation: is it always about personal data?

The GDPR only applies to personal data. Non-personal data therefore falls outside its scope. The legal classification of data is therefore a crucial issue as it determines whether the data processing entity is subject to the various obligations imposed by the Regulation. Yet the binary construction of the European data protection regime, almost 4 years after the entry into force of the Regulation, still does not fully provide the legal certainty that market players desire.

As already mentioned in the previous section, Recital 26 GDPR explicitly states that pseudonymised data are actually personal data[988], whereas it does not take a stance on personal data that have undergone cryptographic techniques, such as encryption. Thus, this section aims to assess the extent to which the distinction between personal and non-personal data is 'dynamic', or rather static, in

---

[983] Stallings and Brown (n 114) 983: in cryptography, a *pepper* is a "random [and secret value] that is concatenated with a password before applying the one-way encryption function used to protect passwords that are stored in the database of an access control system". It differs from *salt,* since the latter is not secret (merely unique) and can be stored alongside the hashed output; Paul A Grassi et al., *Digital Identities Guidelines* (NIST Special Publication, 800-63B, 2017), sec. 5.1.1.2: NIST does not make any formal difference between *salt* and *pepper*, by referring to both as *salt*. The *pepper* value recommended is at least 32 bits: the US agency assures that if the *pepper* value is kept secret, brute-force attacks on the hashed memorised secrets are impractical..

[984] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) 20–21 <http://ec.europa.eu/justice/data-protection/index_en.htm%0Ahttp://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 17 February 2020.

[985] NIST, 'Guide to Storage Encryption Technologies for End User Devices: Recommendations of the National Institute of Standards and Technology' (2007) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf>.

[986] ENISA, 'Recommendations on Shaping Technology According to GDPR Provisions: An Overview on Data Pseudonymisation' (n 978) 17.

[987] Art. 89, recital 156 GDPR.

[988] Recital 26 GDPR: "Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person".

particular, regarding the state-of-the-art of security measures such as encryption and pseudonymisation, provided that it is a moving target[989].

The notion of non-personal data in EU data protection law is not clearly defined. The European Regulation for the free flow of non-personal data (FFDR)[990] provides for a negative definition i.e., "data other than personal data as referred to in Article 4(1) of Regulation (EU) 2016/679"[991]. Therefore, it is necessary to turn our attention at Art. 4(1) GDPR, which states that 'personal data' is "any information relating to an identified or identifiable natural person ('data subject')".

The legal test to assess the 'identifiability criterion' underlying the GDPR's dichotomous architecture, that is, between personal and non-personal data, pivots on Recital 26 GDPR: "[…] To determine whether a natural person is *identifiable*, account should be taken of *all the means reasonably likely to be used*, such as singling out, either *by the controller or by another person* to identify the natural person *directly or indirectly*. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable [emphasis added]".

As a preliminary remark, it should be noted that non-personal data can be divided in two over-arching categories: data that have never been personal, i.e. not relating to an identified or identifiable person, or data that have been personal but were subsequently anonymised. Accordingly, it is possible to look at the categorization of data, i.e. whether personal or non-personal, from a *static* and a *dynamic* perspective. In particular, the latter takes into account "what kind of status modification data can have due to its lifecycle"[992].

Against this background, Recital 26 GDPR sets out the test to be performed to assess how different data processing techniques affect the binary distinction between personal and non-personal data. However, some tenets of Recital 26 created a state of uncertainty as to the interpretation to be given

---

[989] Stefan Schiffner and others, 'Towards a Roadmap for Privacy Technologies and the General Data Protection Regulation: A Transatlantic Initiative' in Manel Medina and others (eds), *Annual Privacy Forum 2018: Privacy Technologies and Policy* (Springer, Cham 2018) 28.

[990] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

[991] Art. 3 FFDR.

[992] Emanuela Podda and Monica Palmirani, 'Inferring the Meaning of Non-Personal, Anonymized, and Anonymous Data' in Victor Rodrìguez-Doncel and others (eds), *AI Approaches to the Complexity of Legal Systems XI-XII. AICOL AICOL XAILA 2020 2018 2020* (Springer International Publishing 2021) 271.

to the grounds of the test; it resulted in diverging views between supervisory authorities and legal scholars.

A closer reading of the text reveals the very essence of the test of Recital 26. Indeed, to establish the identifiability of a person, it is necessary to consider all the means that the controller or any third party may reasonably use to identify that natural person, either directly or indirectly. In order to ascertain the reasonable likelihood of using the means to identify the natural person, all objective factors should be considered, including the costs and time required for identification, taking into account both the technologies available at the time of processing and technological developments.

The test set out in Recital 26 of the GDPR essentially embraces a *dynamic* risk-based approach to determining whether the data is personal or not. Where there is a reasonable risk of identification, the data should be treated as personal data. Where, on the other hand, the risk is negligible, the data may be processed as non-personal data, even if identification cannot be excluded with absolute certainty[993].

This risk-based understanding of the regulation has met with resistance, especially in the so-called 'absolutist' stance[994] adopted by the Article 29 Working Party, which has been followed by some supervisory authorities, such as the French[995] and Irish Data Protection Authorities[996]. This interpretation takes into account all the possibilities and occasions on which anyone would be able to identify the data subject: while the GDPR explicitly refers only to the possibility of identifying ('singling out') the individual, the Working Party goes further, adding to the re-identification test the criteria of (i) *linkability* of information relating to the individual in different datasets; and (ii) *inference* i.e., the possibility of deducing, with significant probability, the value of an attribute from the values of a set of other attributes[997].

As a result, "even theoretical chances of combining data so that the individual is identifiable are included"[998]. Seemingly developing its own 'zero-risk test', the Working Party seeks to equate

---

[993] Finck and Pallas (n 616) 11–36.

[994] Christopher Kuner, *European Data Protection Law : Corporate Compliance and Regulation* (Oxford University Press 2007) 92.

[995] Emanuela Podda and Francesco Vigna, 'Anonymization Between Minimization and Erasure: The Perspectives of French and Italian Data Protection Authorities' in Andrea Kö and others (eds), *Electronic Government and the Information Systems Perspective: 10th International Conference, EGOVIS 2021* (Springer International Publishing 2021) 109 <http://dx.doi.org/10.1007/978-3-030-86611-2_8>; CNIL, 'L'anonymisation de Données Personnelles ' (2020) <https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles> accessed 5 May 2022.

[996] Data Protection Commission, 'Guidance on Anonymisation and Pseudonymisation' (2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614 Anonymisation and Pseudonymisation.pdf> accessed 5 May 2022.

[997] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 984) 3.

[998] Gerald Spindler and Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 163, 165.

anonymisation with erasure in terms of reversibility[999]. However, the flourishing literature on the non-absolute and *dynamic* character of anonymisation[1000] – due to technical advancements – makes it difficult to uphold the Working Party's interpretation.

By following the 'zero-risk test', we could not rely on widely used anonymisation techniques (such as k-anonymity or differential privacy[1001]), since these do not – in absolute terms – exclude the risk of re-identification[1002]. It follows that any information would always remain within the scope of the GDPR, making data protection law 'the law of everything'[1003]. Therefore, when it comes to assessing cryptographic techniques, according to the absolute approach, if *anyone* is *theoretically* able to decrypt the dataset, then "the operations of the controller or processor using this encrypted data are subject to data protection legislation, even if they don't possess the key for decryption"[1004].

Another interpretation of Recital 26, the so-called relativist reading, considers only the efforts required to identify an individual, without entering the murky field of mere theoretical possibilities[1005]. Several authors[1006] and the UK Data Protection Authority, the Information Commissioner's Office (ICO), have argued that data resulting from anonymisation operations by means of cryptographic techniques should not be considered personal data if two requirements are met: the cryptographic

---

[999] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 984) 6.

[1000] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA l. Rev. 1701; L Sweeney, 'Simple Demographics Often Identify People Uniquely' (2000) 3; Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymization of Large Sparse Datasets', *Proceedings - IEEE Symposium on Security and Privacy* (2008).

[1001] Ugo Pagallo, 'The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection' (2017) 3 European Data Protection Law Review 36, 37. The author states that Apple mastered such techniques in order to process health data for statistical purposes, to which the GDPR's regime does not apply. In particular, having regard to the anonymisation process for statistical purposes, see EDPS, 'EDPS Opinion on Safeguards and Derogations under Article 89 GDPR in the Context of a Proposal for a Regulation on Integrated Farm Statistics ' (2017) <https://edps.europa.eu/data-protection/our-work/publications/opinions/farm-statistics_en> accessed 1 June 2022; Inge Graef, Raphael Gellert and Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation' (2020) 44 European Law Review 605, 613: "even when organisations are only in possession of aggregate statistical data and the initial identifiers have been destroyed, such data might still be considered personal depending upon whether it has been subjected to anonymisation techniques, and whether the latter are considered adequate".

[1002] ENISA, 'Data Protection Engineering: From Theory to Practice' (n 975) 10–13; Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279.

[1003] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40; Raphaël Gellert, 'Personal Data's Ever-Expanding Scope in Smart Environments and Possible Path(s) for Regulating Emerging Digital Technologies' (2021) 11 International Data Privacy Law 196.

[1004] Spindler and Schmechel (n 998) 165.

[1005] ibid 166.

[1006] Samson Yoseph Esayas, 'The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules : Beyond the "All or Nothing" Approach' (2015) 6 European Journal of Law and Technology 1.

method must be effective, robust and up-to-date and the data controller (or any third party) is not in possession of the decryption key, nor is there any reasonable possibility of them obtaining the key[1007].

In particular, the ICO did not seemingly change its view from the 2012 guidance. In the draft report on anonymisation and pseudonymisation of 2021 – to be published in 2022 after a public consultation – the DPA explicitly confirms the 'relativist' approach by stating that "the same information can be personal data to one organisation, but anonymous information in the hands of another organisation. Its status depends greatly on its circumstances, both from your perspective and in the context of its disclosure"[1008]. Besides the potential applications in the field of cloud computing[1009], when applied to cryptography, this approach would lead to interesting results[1010]. If the cryptographic method adopted is suited to the data processing at stake and up-to-date and the data controller is either not in possession of the decryption key or has no reasonable chances of obtaining the key, then the data which result from that processing should not be considered as personal data[1011].

Interestingly, the Working Party arguably shares this approach in the 2007 'Opinion on the concept of personal data': if appropriate technical measures such as irreversible hashing have been put in place, "even if identification of certain data subjects may take place despite all those protocols and measures (due to unforeseeable circumstances such as accidental matching of qualities of the data subject that reveal his/her identity), the information processed by the original controller may not be considered to relate to identified or identifiable individuals taking account of all the means likely reasonably to be used by the controller or by any other person"[1012]. The conflict between the two Opinions of the Working Party 29 is real, and all bear witness to the complexity of the arguments at stake.

However, the most convincing position is the one based on the risk approach, which inspired the Regulation and has been confirmed by the CJEU, which seems to have distanced itself from the *YS*[1013]

[1007] Information Commissioner's Office, 'Anonymisation: Managing Data Protection Risk Code of Practice' (2012) 66 <https://ico.org.uk/media/1061/anonymisation-code.pdf> accessed 6 May 2022.

[1008] Information Commissioner's Office, 'Introduction to Anonymisation' (2021) 9 <https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf> accessed 6 May 2022.

[1009] W Kuan Hon, Christopher Millard and Ian Walden, 'The Problem of "Personal Data" in Cloud Computing: What Information Is Regulated?—The Cloud of Unknowing' (2011) 1 International Data Privacy Law 211.

[1010] Chiara, 'Disentangling Encryption from the Personalization Debate: On the Advisability of Endorsing the "Relativist Approach" Underpinning the Identifiability Criterion' (n 247).

[1011] Esayas (n 1006) 8–9; Patrick Lundevall-unger and Tommy Tranvik, 'IP Addresses – Just a Number?' (2011) 19 International Journal of Law and Information Technology 53.

[1012] Article 29 Data Protection Working Party, 'Opinion 04/2007 on the Concept of Personal Data' (2007) 20.

[1013] Joined Cases C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* [2014] ECLI:EU:C:2014:2081. In essence, the Court in YS stated that if the information under scrutiny cannot be corrected and accessed then it cannot be considered as personal data.

jurisprudence[1014]. In the seminal *Breyer* case[1015], the CJEU confirmed the risk-based approach as the Court carried out an evaluation on the actual risk of identification[1016]. The judges of Luxembourg considered the dynamic IP address of Mr. Breyer as personal data even if the additional data necessary for identification of the subject were not held by German authorities i.e., the data controller in said scenario, but by the internet service provider, therefore, a third party[1017]. This stance dismisses a *pure* relativist approach, as "there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person"[1018].

If there is a reasonable likelihood that certain data, even if subjected to irreversible encryption operations to achieve anonymisation (e.g., salted/peppered hash function), can be (re-)linked to the natural person they originally referred to, they must be qualified as personal data. On the other hand, if de-identification has been sufficiently robust that identification is no longer reasonably likely, that data must be considered as non-personal[1019]. To this end, determining the resources (e.g., in terms of time and money) that are needed for a successful re-identification is key to effectively adhere to the concept of risk management. For instance, Finck and Pallas calculated the time and energy costs that are 'reasonably likely' to be spent to carry out a successful reidentification (through brute-force attack) on cryptographic hash functions, such as SHA-3[1020]. They conclude that the adoption of SHA-3, with an appropriate pepper length (such as 32 bits), "would lead to more than 140 years with 10,000 current GPUs"[1021], an effort that cannot possibly be deemed as 'reasonably likely'.

As a consequence, that data should fall outside the GDPR's scope: "if data can be matched to a natural person with reasonable likelihood, it qualifies as personal data and falls within the GDPR's scope of application. If de-personalisation has been sufficiently strong so that identification is no longer reasonably likely, this is non-personal data and accordingly falls outside the Regulation's scope of

---

[1014] Gabriela Zanfir-Fortuna, 'Personal Data for Joint Controllers and Exam Scripts' (2018) 2 International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel 12, 17.

[1015] Case C-582/14 (n 616).

[1016] Frederik Zuiderveen Borgesius, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (2017) 3 European Data Protection Law Review 130.

[1017] Case C-582/14 (n 616), para. 49.

[1018] *Ibid.*, para. 43; see also Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013) 31 <http://ec.europa.eu/justice/data-protection/index_en.htm> accessed 6 May 2022: "a very significant grey area, where a data controller may believe a dataset is anonymised, but a motivated third party will still be able to identify at least some of the individuals from the information released".

[1019] EDPS and AEPD (n 969).

[1020] Morris J Dworkin, 'SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions' (2015) § V <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf> accessed 10 May 2022: this standard will "[p]rovide resilience against future advances in hash function analysis, because they rely on fundamentally different design principles. In addition to design diversity, the hash functions in this Standard provide some complementary implementation and performance characteristics to those in FIPS 180-4".

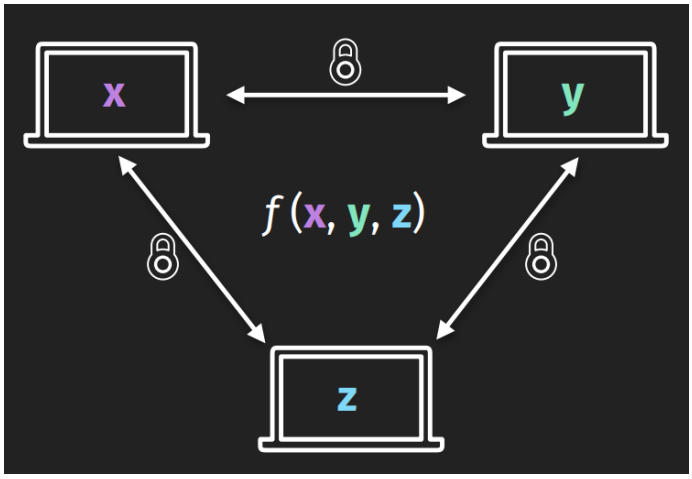
[1021] Finck and Pallas (n 616) 26.

application"[1022]. The EDPS and AEPD (Spanish Agency for Data Protection) ended up with the same result, albeit with a more cautious approach[1023]. In conclusion, a sound technical risk assessment – pivoting on solid technical assumptions based on actual calculations – is needed to ascertain the extent to which re-identification is reasonably likely; this informed and justifiable process would satisfy *inter alia* the principle of accountability.

4.2.3 Encryption's inherent conflict, amidst inbuilt vulnerabilities and innovative methods to uphold fundamental rights

The previous section expressly acknowledges encryption as natural means of data protection and information security. Nevertheless, the inherent dependency on allegedly trusted third parties for key management and certification creates (new) vulnerabilities – in addition to the ones that the very same technologies scrutinised aim to mitigate – that necessitate "further digital security technologies to detect fraudulent third parties or attacks against trusted platforms"[1024]. Thus, this section, building on the outcomes of the previous legal analysis, dwells on different state-of-the-art cryptographic protocols with a view of addressing i) the legal classification of data being processed by these cryptosystems; ii) trust and privacy – understood by proxy as confidentiality – issues in the specific context of (resource-constrained) IoT devices.

The first cryptosystem under investigation is (secure) multi-party computation (SMPC). An SMPC allows many parties to collectively evaluate an aggregate function on the data they all – separately – provided, and learn the output of the function, without revealing and learning anything beyond their own inputs and outputs to any other party[1025].



[1022] ibid 34.

[1023] EDPS and AEPD (n 969) 17–18.

[1024] Hildebrandt (n 183) 262.

[1025] Peeter Laud and others, 'Basic Constructions of Secure Multiparty Computation' in Peeter Laud and Liina Kamm (eds), *Application of Secure Multiparty Computation* (IOS Press 2015) 1.

Figure 8: SMPC protocol[1026]

SMPC can be achieved through *threshold* and *somewhat* homomorphic encryption. The former method allows a secret value to be revealed to any set of at least *x* parties, while revealing no information about that value to any set smaller than *x*. One party will be able to decrypt if it knows at least *x* out of the many decryption keys (*n*). "Computation on homomorphic encryptions can be performed by the *n* parties holding the decryption keys for the cryptosystem"[1027]. The difference between 'somewhat homomorphic encryption' is that the latter only supports a finite number of sequential calculations[1028]. Similarly, SMPC can be based on *Shamir's secret sharing*[1029] scheme, which "allows a value to be shared among *n* parties so that certain coalitions of them can recover it from their shares, and certain other, smaller coalitions obtain no information about that value from their shares. Most frequently, there is a threshold *t*, so that all the coalitions with a size of at least *t* can find the value, and no coalition smaller than *t* gets any information"[1030].

Polymorphic encryption is yet another cryptosystem that is worth analysing[1031]. The Polymorphic Encryption and Pseudonymisation (PEP) model, designed by Verheul, Jacobs, Meijer, Hildebrandt and de Ruiter, is a novel approach to the management of sensitive personal data, in the health care sector, which provides for the necessary security and privacy & data protection infrastructure for big data analytics where there are multiple sources of personal data[1032], like in IoT scenarios. The starting point is the assumption that traditional encryption is rather rigid, as there is only 'one key' able to decipher the encrypted information. This approach hinges on encrypting 'at the source', that is, directly after the generation of personal data and decisions about who can decrypt are therefore postponed. Personal data transfer and storage at cloud facilities is thus secure and the cloud provider cannot gain access to the encrypted data as it does not hold the keys.

The data subject is placed at the centre of the processing, as they play a crucial role in deciding who can decrypt such data, according to a proactive approach towards data protection similar to the one seen with transparency enhancing tools. The chosen party (e.g., a doctor, a medical researcher, etc.)

[1026] Michael Veale, 'Knowing without Seeing: Informational Power, Cryptosystems and the Law' (2019) 3 <https://suri.epfl.ch/slides/2019/michael-veale.pdf>.

[1027] Laud and others (n 1025) 13.

[1028] ibid 15.

[1029] Adi Shamir, 'How to Share a Secret' (1979) 22 Communications of the ACM 612 <https://dl.acm.org/doi/abs/10.1145/359168.359176> accessed 17 May 2022.

[1030] Laud and others (n 1025) 10.

[1031] Chiara, 'Disentangling Encryption from the Personalization Debate: On the Advisability of Endorsing the "Relativist Approach" Underpinning the Identifiability Criterion' (n 247).

[1032] Eric Verheul and others, 'Polymorphic Encryption and Pseudonymisation for Personalised Healthcare' (2016) <https://pep.cs.ru.nl/>.

will be provided with a unique private key, generated from the user's private master key *x,* which is securely stored at a trusted Key Server. An intermediary, the 'tweaker', then grants access to the chosen parties by *re-keying* the encrypted data with the public master key *x* without knowing *x,* and thus working blindly. It cannot access the information it is giving access to[1033]. The Tweaker is "a central converter who exclusively knows how to turn the wheel on a polymorphic lock so that keys of specific parties fit"[1034]. The Tweaker also assigns *local* pseudonyms. Each data subject will have a different pseudonym at different parties, since "[t]hese parties could somehow lose their data, or even maliciously combine data with others. If different parties use different pseudonyms for the same patient, it is in principle not possible to combine the data, at least not on the basis of identifiers"[1035].

Using this innovative approach, a lightweight cryptosystem based on polymorphic encryption has been proposed to secure both hardware and the data flow associated with IoT resource-constrained devices. The implementation of a cryptosystem as flexible as the polymorphic encryption – which is resistant to the most common attacks – at the hardware level would ensure better security and performance than the software implementation[1036].

There may be reasons to consider the data resulting from computations performed by complex cryptosystems, such as the above mentioned, as non-personal data. Some argue that in specific scenarios, such as the healthcare-domain, "multi-party computation has the potential to fulfil the requirements for computational anonymity by creating anonymised data in a way that does not allow the data subjects to be identified with means reasonably likely to be used"[1037].

Others, in turn, analysed the possible outcomes in terms of personal or non-personal data by applying the relative and absolute approaches (in Recital 26 GDPR) to several SMPC use-cases[1038]. The range of results contemplated by the authors is not binary i.e., personal or non-personal data, and thus application or non-application of the GDPR, but they also include the outcome 'SMPC as a data protection by design measure' as they consider scenarios where SMPC effectively minimises personal data output. Yet, in the latter case, the information resulting from the SMPC would still be personal data.

[1033] ibid 8.

[1034] ibid 7.

[1035] ibid 11.

[1036] Indira Kalyan Dutta and others, 'Lightweight Polymorphic Encryption for the Data Associated with Constrained Internet of Things Devices', *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)* (IEEE 2020) 6.

[1037] Gerald Spindler and Anna Zsófia Horváth, 'SODA Project: D3.5 Use-Case Specific Legal Aspects' (2019) 63 <https://cordis.europa.eu/project/id/731583/results/it>; Spindler and Schmechel (n 998) 176.

[1038] Lukas Helminger and Christian Rechberger, 'Multi-Party Computation in the GDPR', *Privacy Symposium 2022 - Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT)* (2022).

All in all, to assess whether the output data of a cryptosystem is personal or not, a sound technical (i.e., calculation) risk assessment must be carried out to ascertain the extent to which re-identification of previously de-identified personal data, using state-of-the-art anonymisation techniques, is reasonably likely, as the preceding section has shown[1039]. "Saying cryptosystems such as these do not legally process personal data will usually be a shaky argument"[1040].

While it may recall a relativist understanding of the identifiability test[1041], the case of polymorphic encryption in particular might be seen as a compelling argument for claiming that digital security technologies, such as encryption, are paradoxically not neutral vis-à-vis fundamental rights as they generate new digital security risks. Thus, cryptosystems rely on "trusted third parties for key management and certification [:] to the extent that trust is intransitive and does not scale, this implies that encryption generates new vulnerabilities that require further DSTs to detect fraudulent third parties or attacks against trusted platforms"[1042].

It follows that the higher the number of keys, the higher the risk. In polymorphic encryption, the number of keys for the polymorphic 'locks' of the parties granted to decrypt and process the personal data by the user is potentially unlimited[1043]. If the trusted Key Server (that holds the master private key) and the Tweaker (that holds the key factors for re-keying and therefore decrypting) collude, the system breaks down[1044].

On the one hand, one has to acknowledge the ineradicable dependency relationship between risk and trust: where there is trust, there is always a degree of risk[1045]. On the other hand, organisational and technical measures can be adopted to reduce the risk of collusion. Besides organisational measures such as data and physical access control, entry logs, availability control and cybersecurity and data protection educational trainings, contractual arrangements or non-disclosure agreements between the parties aiming at avoiding re-identification are often included in any legal framework for the anonymisation of personal data.

[1039] Chiara, 'Disentangling Encryption from the Personalization Debate: On the Advisability of Endorsing the "Relativist Approach" Underpinning the Identifiability Criterion' (n 247) 183.

[1040] Veale (n 1026).

[1041] A party, such as a cloud service provider, only receives data encrypted at the source and cannot access the plaintext unless the Tweaker grants it the keys.

[1042] Hildebrandt (n 183) 262.

[1043] Verheul and others (n 1032) 7.

[1044] Eric Verheul and Bart Jacobs, 'Polymorphic Encryption and Pseudonymisation' (2017) 5 NAW 168, 170 <http://www.ecc-brainpool.org> accessed 17 May 2022.

[1045] Durante, 'Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks' (n 301) 380.

Furthermore, technical means adopted for data fragmentation, such as 'secret sharing' security protocols[1046], can arguably lower the risk of potential collusions; the *trust* in the system would increase accordingly. A secret sharing scheme is highly flexible: combined with other cryptographic techniques such as SMPC, it may be applied to personal data sets after the acquisition and prior to the analysis (at cloud level, say) phases by dividing personal data into unintelligible and random 'shares' that will end up in different servers, enabling multi-party computation on those 'shares'[1047]. Such complex cryptographic architectures aim to give the data subject (the patient, in the health care domain) "total control over the generation and management of the decryption keys without relying on a trusted authority"[1048] and thus are particularly suitable for cloud environments.

However, there is no silver bullet for information and network security. Risk is the unavoidable flip side of trusting (or relying on) technical means such as cryptosystems. In particular, the next section explores several privacy-invasive scenarios vis-à-vis IoT metadata analysis, even if the communication is encrypted, and introduces the applicable legal framework under EU law.

4.3 Privacy Risks despite Encryption: IoT Metadata Analysis and the EU Privacy and Data Protection Legal Frameworks

Notwithstanding the lightweight – in case of resource-constrained devices - or 'strong' encryption protocols that may be adopted to secure (IoT) device communication, serious privacy concerns nevertheless arise as an adversary can draw inferences related to user activity by relying on some properties of metadata accompanying the encrypted data. Thus, encrypted traffic analysis, i.e., metadata analysis, is definitely a hot topic in the search to secure IoT users' privacy[1049]. Against the background of the last three legal challenges identified by the Article 29 Working Party in its Opinion on the IoT[1050], section 4.3.1 casts light on state-of-the-art attacks and eavesdropping techniques on encrypted traffic that enable granular profiling and surveillance in terms of habits and behavioural patterns. Section 4.3.2 addresses the main legal instruments of EU privacy and data protection law that can be adopted to tackle the challenges raised in the previous section.

[1046] Katz and Lindell (n 967) 501–507.

[1047] Ismail and others (n 249); Spindler and Horváth (n 1037) 48–56.

[1048] Ismail and others (n 249) 250.

[1049] Rayes and Salam (n 13) 235.

[1050] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 851) 7–8. The challenges are: i) inferences derived from data and repurposing of original processing; ii) intrusive bringing out of behaviour patterns and profiling; and, iii) limitations on the possibility to remain anonymous when using services.

4.3.1 Device and user identification: an overview of fingerprinting and inferencing techniques

As consistently emphasised throughout this work, in the dawn age of IoT's hyper-connection, data reuse and data mining, it will become increasingly arduous to discern whether data or metadata "does and does not and will likely not impact" individuals' fundamental rights[1051], amid increasingly easier way to single out an individual on very few data points[1052].

Despite the adoption of transport layer encryption, the cybersecurity measure *par excellence* in the field of data protection and information security[1053], IoT traffic metadata (which is not encrypted) is enough for a motivated passive network adversary to infer either users' activities or devices states and possibly obtain sensitive information[1054]. The concept of 'fingerprinting' refers to the possibility of creating data records which map certain properties of the encrypted data observed to the corresponding files, website or device: "given a corresponding data base of fingerprints, it is possible to find a match in the database of fingerprints and thus perform file or website identification even on encrypted traffic"[1055].

File and website fingerprinting can be subsumed under the broad category of network metadata analysis. Website fingerprinting aims at identifying which website, or part thereof, a user is browsing, by looking only at the user's encrypted traffic[1056]. However, for the purpose of this section, 'files fingerprinting' and 'device identification' – especially in the context of smart environments – are the categories that most deserve our attention.

File fingerprinting, through the adoption of machine learning algorithms (such as decision trees and random forests)[1057], allows for the detection of known data, even in real-time, in encrypted

---

[1051] Inge Graef and others, 'Feedback to the Commission's Proposal on a Framework for the Free Flow of Non-Personal Data' [2018] SSRN Electronic Journal 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3106791> accessed 17 February 2020.

[1052] EDPS, 'EDPS Comments on a Framework for the Free-Flow of Non-Personal Data in the EU ' (2018) 3 <https://edps.europa.eu/data-protection/our-work/publications/comments/edps-comments-framework-free-flow-non-personal-data_en> accessed 3 June 2022.

[1053] See section 4.2.

[1054] Noah Apthorpe and others, 'Keeping the Smart Home Private with Smart(Er) IoT Traffic Shaping' (2019) 3 Proceedings on Privacy Enhancing Technologies 128; Abbas Acar and others, 'Peek-a-Boo: I See Your Smart Home Activities, Even Encrypted!' [2020] WiSec 2020 - Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks 207; Jingjing Ren and others, 'Information Exposure from Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach' [2019] Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC 267.

[1055] ENISA, 'Encrypted Traffic Analysis: Use Cases & Security Challenges' (2020) 27 <https://www.enisa.europa.eu/publications/encrypted-traffic-analysis>.

[1056] Andriy Panchenko and others, 'Website Fingerprinting at Internet Scale', *NDSS* (2016); Payap Sirinam and others, 'Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning', *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (ACM 2018).

[1057] Roberto Casarin and others, 'Decision Trees and Random Forests' in Mohammad Zoynul Abedin and others (eds), *The Essentials of Machine Learning in Finance and Accounting* (1st edn, Routledge, Taylor and Francis Inc 2021).

communication channels with high accuracy[1058]. In the context of IoT-surveillance, AI algorithms (e.g., random forest classification model) have proven to be useful in the analysis of encrypted video content. Based on the statistical characteristics of encrypted traffic, a ML model can classify the user behaviour underlying the surveillance video traffic, provided that the traffic patterns of cloud monitoring cameras differ significantly when users do different activities on their monitoring screens[1059].

Device identification could even shed more light on the sensitivity of IoT metadata. As said, through sniffing techniques, an eavesdropper can observe the traffic rate, network protocols, source and destination addresses, packets sizes and header metadata[1060] of the network traffic[1061]. As was the case with the other types of fingerprinting, the monitoring of the network traffic is functional to feeding machine learning algorithms[1062] that extract different device features (e.g., timing, sensor state, device state, controller state, controller location) from the encrypted traffic, enabling the accurate identification of the interactions that caused the network traffic[1063]. In other words, "an eavesdropper can reliably learn a user's interactions with a device across a wide range of categories, opening the potential for profiling and other privacy-invasive techniques"[1064].

After device identification, *via* fingerprinting, a motivated tech-savvy adversary may infer valuable information, such as the timing of user activities from changes in traffic rates, correlated to device state changes. "Most user interactions with IoT devices occur at discrete time points or over short periods surrounded by extended periods of no interaction. For example, turning on a lightbulb, falling asleep, querying a personal assistant, and measuring blood pressure do not occur continuously"[1065].

[1058] Konstantin Böttinger, Dieter Schuster and Claudia Eckert, 'Detecting Fingerprinted Data in TLS Traffic', *ASIACCS 2015 - Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (Association for Computing Machinery 2015) 633–638.

[1059] Jibao Wang and others, 'User Behavior Classification in Encrypted Cloud Camera Traffic', *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings* (Institute of Electrical and Electronics Engineers Inc 2019).

[1060] Data packets communicated (transport layer) from the IoT system to the server are sent with so-called timestamps, i.e., the time and date of the action delivered by the device: in case of aggregated timestamps, one can retrieve timing patterns.

[1061] Noah Apthorpe, Dillon Reisman and Nick Feamster, 'A Smart Home Is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic' [2017] arXiv <https://arxiv.org/pdf/1705.06805.pdf> accessed 3 June 2022.

[1062] Such as decision trees, random forests and naïve bayes.

[1063] Acar and others (n 1054).

[1064] Ren and others (n 1054) 276–277.

[1065] Noah Joseph Apthorpe, 'Network Privacy and User Protection in the Internet of Things' (Princeton University 2020) 192–193 <https://search.proquest.com/dissertations-theses/network-privacy-user-protection-internet-things/docview/2427502325/se-2?accountid=13042%0Ahttp://oxfordsfx.hosted.exlibrisgroup.com/oxford?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&g>.

Moreover, the observer could infer sensitive information about the states, the actions, the types of smart devices and sensors as well the related user activities[1066]. "The limited-purpose nature of most IoT devices makes this possible. Users interact with traditional computing devices, such as PCs and smartphones, for a variety of purposes, making it difficult to associate any particular change in network traffic rate with a specific activity. In comparison, once an attacker has identified the identity of a particular IoT device, it is often trivial to associate specific traffic rate changes with user activities"[1067].

Unlike web browsing, IoT devices generally communicate with few servers, mainly operated by manufacturers, and only one, non-overlapping flow of network traffic is usually needed to perform activity inference. "Additionally, many devices queried individual domains that uniquely identify the device or manufacturer without requiring the use of a set-based fingerprint. This ability to fingerprint based on destination IP addresses is specific to the IoT setting"[1068].

In real world scenarios, machine learning models, such as the ones described above, if trained on a small set of devices, would not work on a large set of unknown IoT devices. A solution has been proposed to keep the model updated with local data and perform regular neural network-based models retraining at the edge, rather than at the cloud server level[1069]. It follows that IoT devices can be identified based on their network behaviour, using resources available on devices themselves (i.e., at the edge of the network). In other words, the accurate and automated inference of the category of a newly connected IoT device to a network, albeit fairly complex, is feasible.

Conventional technical solutions to the identified problem are hardly applicable to IoT scenarios. Protecting metadata with cryptographic means, claimed elsewhere as a possible mitigation against Internet service providers' privacy invasive activities[1070], would require too much computational power for devices that are mostly constrained. It follows that they are not suited to deploying anonymous communication systems like The Onion Router (TOR) which are highly demanding in terms of processing and storage capacity. Similarly, firewalls and virtual private networks (VPN) may

---

[1066] Nazanin Takbiri and others, 'Matching Anonymized and Obfuscated Time Series to Users' Profiles' (2019) 65 IEEE Transactions on Information Theory 724.

[1067] Apthorpe (n 1065) 193.

[1068] ibid 194.

[1069] Roman Kolcun and others, 'Revisiting IoT Device Identification', *Network Traffic Measurement and Analysis Conference (TMA)* (2021) <https://arxiv.org/pdf/2107.07818.pdf> accessed 11 May 2022.

[1070] Wolfgang Schulz and Joris van Hoboken, 'Human Rights and Encryption ' [2016] UNESCO Series on Internet Freedom 22–23 <https://unesdoc.unesco.org/ark:/48223/pf0000246527?1=null&queryId=e05fdd78-68b9-4ff3-b7ce-b998b0c0cf01> accessed 3 June 2022.

severely impact device functionality due to an increase in data usage while still allowing activity inference in certain scenarios[1071].

As a consequence, there is a need for innovative 'lightweight' privacy preserving methods. At a higher level of abstraction, proposed solutions aim to protect IoT traffic rate metadata by obfuscating the (real) user activities with (false) generated traffic patterns[1072]. The vast majority of currently available IoT devices is vulnerable to the inference attacks on privacy described in this section. Without significant changes, in terms of privacy protection techniques to be adopted by manufacturers, this issue will also remain for new classes of IoT devices that are expected to flood our market. On the other hand, adopting proposed privacy-preserving solutions is equivalent to placing a relevant burden on manufacturers' side. Without the right incentives, either at regulatory or market level, IoT manufacturers will likely not develop and deploy such solutions.

4.3.2 'Private surveillance': EU legal frameworks applicable to IoT metadata analysis

The previous section gave an overview of how and to what extent data inference and re-identification could heavily impact individuals' rights to privacy and data protection, potentially leading – in the era of hyper-connection of every-day life objects – "to humiliation or even threat to life due to the disclosure of confidential information"[1073]. Even when state-of-the-art technical safeguards for data security are established, like means of encryption, metadata still retain considerable privacy and data protection implications.

The 2022 ENISA annual report on cybersecurity research & innovation highlights the increasing interest of private and public agents in the surveillance of citizens as a major and cross-sectoral concern. Bolstered by IoT hyperconnectivity, eavesdropping of communications data and metadata could become a major threat, compromising the privacy and protection of users' data[1074]. Without dwelling at length on the legal challenges surrounding 'State surveillance', as an analysis on public and criminal law would exceed the scope of this section, a brief note on the subject is required in order to grasp the extent of the legal debate on metadata processing.

[1071] Apthorpe (n 1065) 187.

[1072] ibid 204–218; Acar and others (n 1054) 11–12; Nazanin Takbiri and others, 'Matching Anonymized and Obfuscated Time Series to Users' Profiles' (2019) 65 IEEE Transactions on Information Theory 724.

[1073] ENISA, 'Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics' (n 979) 13.

[1074] ENISA, 'Research and Innovation Brief: Annual Report on Cybersecurity Research and Innovation' (2022) 14 <https://www.enisa.europa.eu/publications/research-and-innovation-brief>.

From the seminal *Digital Rights Ireland*[1075], which invalidated the contested Data Retention Directive[1076] and *Tele2*[1077] judgments to the more recent *Privacy International*[1078] and *La Quadrature du Net*[1079] cases, the CJEU consistently condemned the *general* and *indiscriminate* retention of metadata to fight serious crime and for national security purposes without appropriate procedural limitations and guarantees according to the proportionality principle. Thus, the CJEU, similarly to the ECtHR[1080], makes it clear that the objectives of protecting national security may legitimise indiscriminate surveillance programmes for as long as necessary to neutralise a *foreseeable* and *concrete* threat to the integrity of the state[1081]. Otherwise, the fight against 'mere' serious crime would only justify measures whose scope is delimited by objective criteria (e.g., geographical, subjective), which must highlight a link between the (meta)data collected and the objectives pursued[1082].

In its caselaw, the CJEU acknowledges that metadata taken as a whole, can afford "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them"[1083]. In other words, metadata analysis may lead to granular profiles of the individuals concerned by such activity, as seen from a technical viewpoint in the previous section.

Leaving aside the issues pertaining to Art. 15(1) of the ePD, in terms of the balancing exercises between protecting fundamental rights and Member States' security needs, the ePD lays down in Art. 5(1) the principle of the confidentiality of communication and related traffic data. National legislation must thus prohibit the listening, tapping, storage or any other ways of surveillance of communications and related traffic data without the consent of the users concerned[1084]. Importantly, after the 2009 revision, the storing of information or the gaining of access to information already stored in the

---

[1075] *Digital Rights Ireland* (n 230).

[1076] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[1077] *Tele2* (n 230).

[1078] *Privacy International* (n 230).

[1079] *La Quadrature du Net* (n 230).

[1080] ECtHR, 25 May 2021, (Application no. 58170/13, 62322/14 and 24960/15), *Big Brother Watch and Others v. United Kingdom*. However, there is a divergence between the two Courts regarding bulk surveillance. *Ex multis* see Maria Tzanou and Spyridoula Karyda, 'Privacy International and Quadrature Du Net: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28 European Public Law 123; Bart Van Der Sloot, 'Big Brother Watch and Others v. the United Kingdom & Centrum För Rättvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?' (2021) 7 European Data Protection Law Review 319.

[1081] *La Quadrature du Net* (n 230) §§ 136-137.

[1082] ibid. §§ 143-148; *Privacy International* (n 230) § 75.

[1083] *Tele2* (n 230) §99.

[1084] Art. 5(1) ePD.

terminal equipment of a user is allowed if the user has given his or her consent[1085], unless the technical storage or access is deemed necessary for i) the transmission of a communication over a network; ii) the provision of a service explicitly requested by the user[1086].

Device fingerprinting, as described in the previous section, would *prima facie* fall outside the scope of the so-called 'cookies provision' enshrined in Art. 5(3). Accordingly, online services would not need users' consent to perform such metadata processing for the purposes of tracking or building profiles for providing analytics.

However, already in 2014, the Article 29 Working Party addressed the relationship between Art. 5(3) and device fingerprinting. Having acknowledged a substantial difference from 'cookies', in that device fingerprinting operates covertly, therefore exacerbating the privacy and data protection risks, the WP concluded that those "device fingerprints which are generated *through the gaining of access to, or the storing of, information on the user's terminal device* must first obtain the valid consent of the user [emphasis added]"[1087].

On the one hand, by bringing into scope the most common use-cases of device fingerprinting at that time, the extensive interpretation of the WP strengthens the standard of protection afforded by the principle of confidentiality of communications as provided for by Art. 5 ePD. On the other hand, AI-powered network analysis of communications metadata – as addressed in the previous section – would not require *per se* the 'gaining of access to, or the storing of, information on the user's terminal device'. It follows that such activities may not be covered by Art. 5(3) ePD. The Italian Data Protection Authority implicitly confirms this interpretation: "the controller uses a reading technique [i.e., device fingerprinting] that *does not require the storage of information within the user's device*, as it only envisages observing the configurations applying to that specific user and making him or her identifiable; the outcome is ultimately a 'profile' that remains in the controller's sole possession, to which the data subject obviously has no free and direct access and of which the data subject might actually be totally unaware [emphasis added]"[1088].

Even if Art. 5(3) would not apply, fingerprinting techniques are likely to fall nonetheless under the scope of the GDPR, to the extent that passive network analysis process data – alone or in combination

---

[1085] Which shall be in accordance with the relevant GDPR provisions.

[1086] Art. 5(3) ePD.

[1087] Article 29 Data Protection Working Party, 'Opinion 9/2014 on the Application of Directive 2002/58/EC to Device Fingerprinting' (2014).

[1088] Garante per la Protezione dei Dati Personali, 'Guidelines on the Use of Cookies and Other Tracking Tools - 10 June 2021' (2021) 21 <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876>.

with others – may lead to the identification of users[1089]. To be lawful, such processing would require a legal basis under Art. 6 GDPR, which may be consent – which would be required if Art. 5(3) applied. Recourse to the GDPR in its role of *lex generalis* should not, however, divert attention away from this regulatory gap in the EU ePrivacy framework, as the GDPR was not meant to address specifically electronic communication networks or communications data – notably including metadata – as such.

In this respect, the focus should now shift towards the relevant provisions of the proposed ePrivacy Regulation. While Art. 5 lays down the general prohibition for anyone to interfere with electronic communications data (including, therefore, metadata) other than the end-users concerned[1090], except when permitted by the Regulation (e.g., Art. 6, see section 4.1), an entire article is devoted to the protection of end-users' terminal equipment information. Art. 8(1) ePR reads: "the use of processing and storage capabilities of terminal equipment and the *collection of information from end-users' terminal equipment, including about its software and hardware,* other than by the end-user concerned shall be prohibited [emphasis added]"[1091]. The broad formulation of the new provision differs significantly from its predecessor: the 'storing/gaining access' standard of the ePD would be enhanced by a more comprehensive 'collection of information from terminal equipment'. It follows that passive information sniffing activities relating to the usage of such terminal equipment in electronic communications networks would fall under the scope of Art. 8 and therefore would only be allowed with the end-users' consent and for specific and transparent purposes.

This interpretation, implicitly confirmed by the Article 29 Working Party[1092] and explicitly by the EDPS[1093] Opinion on the ePR, is underpinned by Recital 20 ePR which directly tackles the problem: "[…] Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users'

[1089] See Art. 4(1); recital 26 GDPR. This would be for example the case of indirectly identifiable MAC addresses of devices.

[1090] EDPB (n 52) 2: "[T]his right to confidentiality must be applied to every electronic communication, regardless of the means by which they are sent, at rest and in transit, from the sender to the receiver, and must also protect the integrity of every user's terminal equipment".

[1091] Art. 8(1) ePR.

[1092] Article 29 Data Protection Working Party, 'Opinion 01/2017 on the Proposed Regulation for the EPrivacy Regulation (2002/58/EC)' (n 874) 9.

[1093] EPDS, 'EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (EPrivacy Regulation)' (2017) 28 <https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf>.

terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific and transparent purposes"[1094].

Against this background, the second paragraph of Art. 8 further substantiates the general prohibition of collecting information *emitted by terminal equipment* for the purposes of connecting to another device or to network equipment but introduces two exceptions. The first derogation is whether the collection is carried out in order to 'establish a connection'[1095]; the second point, which is rather problematic, permits a derogation from the general prohibition if "a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user if the terminal equipment can take to stop or minimize the collection"[1096].

As noticed by the Article 29 WP and the European Supervisor, Art. 8(2)(b) seems to suggest that information related to the terminal equipment may be collected "to track the physical movements of individuals (such as "Wi-Fi-tracking" or "Bluetooth-tracking") without the consent of the individual concerned"[1097], with a mere 'notice' being sufficient. Yet, this exception clashes with the rationale of Recital 20, which strongly states that such activities "may seriously intrude upon the privacy of these end-users"[1098]. Alongside the 'transparency' requirement, the European legislator should consider introducing an obligation for the parties performing surveillance practices to obtain users' consent, as suggested interestingly by both the Council[1099] and the Parliament[1100] in their drafts. As noted by the A29 WP, "only in a limited number of circumstances might data controllers be allowed to process the information emitted by the terminal equipment for the purposes of tracking their physical movements without the consent of the individual concerned"[1101].

[1094] Recital 20 ePR.

[1095] Art. 8(2)(a) ePR.

[1096] Art. 8(2)(b) ePR.

[1097] Article 29 Data Protection Working Party, 'Opinion 01/2017 on the Proposed Regulation for the EPrivacy Regulation (2002/58/EC)' (n 874) 11; EPDS (n 1093) 29.

[1098] Recital 20 ePR.

[1099] Art. 8(2)(b) EU Council ePrivacy Draft.

[1100] Art. 8(2)(b) EU Parliament ePrivacy Draft, amendment 34.

[1101] Article 29 Data Protection Working Party, 'Opinion 01/2017 on the Proposed Regulation for the EPrivacy Regulation (2002/58/EC)' (n 874) 12.

In conclusion, borrowing the words of former European Data Protection Supervisor Giovanni Buttarelli, there is an urgent need for a new ePrivacy law[1102]: four years later, these words are still meaningful, as this section has tried to show.

4.4 Conclusion

This Chapter charted out different privacy & data protection legal challenges brought about by structural IoT data and metadata collection and processing. Drawing on the findings of the Article 29 Working Party's Opinion on IoT, the analysis contributes to the 'IoT privacy debate' by taking into account recent developments from both a technological and regulatory standpoint.

The first legal challenge concerned the realignment of the traditional matters of privacy and data protection that can be observed under IoT data and metadata sharing, and how this structural sharing challenges the two different regimes of the ePrivacy Directive and the GDPR. The first section thus assessed whether relevant provisions of the GDPR, ePrivacy Directive and notably the proposed ePrivacy Regulation are up to the task of coping with the challenges raised by IoT to the traditional notions of consent, transparency and information security.

In the same vein as Chapter 3, the investigation concluded that there is a missing piece in the EU privacy & data protection legislative jigsaw, namely the long-awaited ePrivacy Regulation. However, while the ePrivacy Regulation is much needed to offer end-users a higher standard of protection, alone it will not be enough. Thus, organisational and technological tools (e.g., privacy enhancing technologies, transparency enhancing technologies, privacy preserving technologies, etc.) must be designed to complement the legal protection offered by EU law to individual privacy and data protection.

The second legal challenge hinged on the relationship between various cryptographic technical tools, regarding, but not limited to, encryption, and the traditional legal disciplines of privacy and data protection. Thus, an alignment of privacy, data protection and *cybersecurity* – to be understood broadly so as to cover information security (see Chapter 2) – is particularly striking when it comes to cryptographic technologies that aim to ensure confidentiality.

First of all, the analysis shed light on the rationale and technical pillars of encryption, which substantially differs from hashing and pseudonymisation, and why taking this distinction firmly matters when it comes to data protection. Afterwards, the legal investigation cast light on whether and to what extent state-of-the-art encryption protocols challenge the broad concept of personal data underlying the EU data protection legal framework. It concluded that a sound technical risk

[1102] https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en.

assessment – pivoting on solid technical assumptions based on actual calculations – is needed to ascertain the extent to which re-identification is reasonably likely. Finally, the discussion considered the often-overlooked impact of cryptosystems (such as, secure multi-party computation and polymorphic encryption) on *privacy,* as their reliance on third-parties for key management and certifications generates new vulnerabilities. To mitigate the risks of internal (i.e., collusion) and external attacks, the analysis mapped out several organisational and technical measures. On the one hand, contractual arrangements (e.g., non-disclosure agreements), data and physical access control, entry logs, availability control and cybersecurity and data protection educational training have been included. On the other hand, to lower the risk of potential collusions between trusted parties, technical means for data fragmentation, such as 'secret sharing' security protocols, have been proposed.

Notwithstanding the lightweight – in the case of resource-constrained devices – or 'strong' encryption protocols that may be adopted to secure (IoT) device communication, serious privacy concerns nevertheless arise as an adversary can draw inferences related to user activity by relying on some properties of metadata accompanying the encrypted data. Against this background, the last legal challenge, that is, IoT metadata analysis, cast light on state-of-the-art attacks and eavesdropping techniques on encrypted traffic enabling granular profiling and surveillance.

After the technical overview, the investigation addressed the relevant provisions of the ePrivacy Directive and the proposed ePrivacy Regulation that can tackle the above-mentioned challenge, in particular, having regard to device fingerprinting. It concluded that the long-awaited ePrivacy Regulation would strengthen and enhance users' privacy protection vis-à-vis passive network analysis compared to the existing legal framework, as set out in Art. 5(3) of the Directive, which may not cover AI-powered network analysis on communications metadata. Despite this, the broad formulation of Art. 8 of the Regulation, which would cover 'sniffing' passive network activities, needs to be streamlined in order to avoid introducing derogations from the principle of obtaining users' consent for the companies performing surveillance practices even if clear and prominent notices are displayed to inform the users where data are collected.

Chapter 5. Holistic Risk Analysis for IoT

5.1 Risk Assessment in EU Data Protection and Cybersecurity: Similarities and Divergences

5.1.1 The Data Protection Impact Assessment 'risk to rights' approach

Risk management has always been an essential element of data protection regulations[1103]. With the emergence of new technologies and the increasing complexity of data processing scenarios, the EU legislator introduced new specific risk management provisions to modernise the EU data protection legal framework, notably Articles 35 and 36 GDPR. "This has shifted the focus of data protection regulation away from the legitimacy of data processing and the data subject's self-determination to the controllers' accountability and risk management"[1104]. In particular, the principle of accountability (Art. 5(2) GDPR) reflects the GDPR co-regulative model of governance, according with which data controllers shall be able to prove compliance with the principles relating to personal data processing enshrined in Art. 5(1)[1105].

Hence, Art. 24 and 25(1)[1106] further substantiate the nature and scope of such improved responsibility of controllers. To effectively comply with the GDPR, controllers have to take organisational and technical measures to meet the requirements of the law, taking into account, *inter alia*[1107], the risks of varying likelihood and severity to the rights and freedoms of the individuals concerned. "The risk-

[1103] Raphael Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016) 2 European Data Protection Law Review 481.

[1104] Alessandro Mantelero, 'Comment to Articles 35 and 36' in Mark D Cole and Franziska Boehm (eds), *GDPR Commentary* (Edward Elgar Publishing, forthcoming) 8 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362747>.

[1105] Pagallo, Casanovas and Madelin (n 209) 9.

[1106] Art. 25 enucleates the principles of data protection by design and by default. The former is embodied in Art. 25(1) which requires data controllers to integrate the necessary safeguards – by means of organisational and technical measures – into the processing, both at the time of the determination of the means for processing and at the time of the processing itself, in order to meet the principles and requirements of this Regulation and protect the rights of data subjects. 'Data Protection by default' is instead substantiated by Art. 25(2) as controllers must 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. See *ex multis* Giorgia Bincoletto, *Data Protection by Design in the E-Health Care Sector*, vol 22 (Luxembourg Legal Studies, Nomos 2021).

[1107] Articles 24 and 25(1) make reference to the state-of-the-art, the cost of implementation and the nature, scope, context and purposes of processing.

based approach to data protection lies in the use of this notion of risk so as to enable controllers to implement abstract legal norms in an appropriate and effective manner"[1108].

Provided that the normative architecture of the GDPR is structured around the notion of risk, the question that now should be asked is what kind of *risk* does the GDPR address? In his seminal work, Gellert argues that the GDPR is about 'compliance risk': following a traditional understanding of risk being composed of an event and its consequences, the GDPR would envisage the lack of compliance as the 'event', whereas the 'consequence' arising from the event would be the risks to the data subjects' rights and freedoms[1109]. In other words, the lower the compliance the higher the consequences upon the data subjects' rights.

Against this backdrop, Art. 35 GDPR provides for the obligation to carry out data protection impact assessments (DPIAs), a risk management iterative process to be performed by the controller prior to processing which is likely to result in a "high risk to the rights and freedoms of natural persons"[1110]. In a similar vein to Art. 24(1) and 25(1)[1111], the DPIA shall be regarded as the culmination of the accountability principle rooted in the risk-based approach[1112]. Thus, the controller – after having received advice from the data protection officer (DPO)[1113] – needs to evaluate whether a particular type of processing may entail such 'high risk to the rights and freedoms' "by taking into account the nature, scope, context and purposes of the processing"[1114], particularly if it makes use of new technologies. The processor might only be involved in assisting the controller in carrying out a DPIA *via* contractual means and if it performs all or part of the processing[1115].

The reference to 'rights and freedoms' deserves careful attention. Even if the GDPR impact assessment hinges on data protection, as we are reminded by the heading of Art. 35, the risks that ought to be considered by the controller do not concern solely privacy and data protection rights but all the fundamental rights that may be impacted by the processing under scrutiny[1116]. Section 5.1.3

[1108] Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502, 503.

[1109] Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (n 1002).

[1110] Art. 35(1) GDPR.

[1111] Eleni Kosta, 'Article 35 Data Protection Impact Assessment' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 669–670.

[1112] Athena Christofi and others, 'Erosion by Standardisation: Is ISO/IEC 29134:2017 on Privacy Impact Assessment up to (GDPR) Standard?', *Research Anthology on Privatizing and Securing Data* (IGI Global 2021) 6. See also recital 84 GDPR.

[1113] Art. 35(2); 39(1)(c) GDPR.

[1114] Art. 35(1) GDPR.

[1115] Art. 28(3)(f) GDPR.

[1116] Dara Hallinan and Nicholas Martin, 'Fundamental Rights, the Normative Keystone of DPIA' (2020) 6 European Data Protection Law Review 178; Kosta, 'Article 35 Data Protection Impact Assessment' (n 1111) 671; Mantelero, 'Comment to Articles 35 and 36' (n 1104) 8.

will further elaborate on this often neglected point when Art. 35 is operationalised, as DPIA models offered by the DPAs fail to offer a comprehensive account of risks to a broader set of rights than privacy and data protection.

The GDPR enucleates only three specific cases of 'risk-to-rights' processing operations. The non-exhaustive list[1117] of Art. 35(3) contains:

1. "Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person", the effect of which potentially being exclusion or discrimination;
2. Processing on a large scale of special categories of data or personal information relating to criminal convictions and offences;
3. large- scale extension of systematic monitoring of publicly accessible areas.

Beside these cases, if it is not clear whether a DPIA is required, the WP29 guidelines recommend performing the assessment nonetheless "as a DPIA is a useful tool to help controllers comply with data protection law"[1118]. On the other hand, throughout the legal standard of Art. 35 'exemptions' to such rule of thumb can be found. A DPIA is not required where i) a processing is not likely to result in high risk[1119]; ii) a DPA establishes that a particular processing would not require a DPIA[1120]; iii) where the legal basis of a processing is to be found in Art. 6(1)(c) or Art. 6(1)(e) GDPR and the relevant law regulates such processing and a DPIA has already been carried out as part of a general assessment in the context of the adoption of the legal basis[1121].

Yet, Recital 75 is in itself a significant contribution to shedding light on the meaning of 'risk to rights and freedoms'. It identifies six criteria to assess the risk, of varying likelihood and severity, for the rights and freedoms of natural persons that may result from personal data processing which could lead to physical, material or non-material damage[1122]. In other words, "it contains several risk criteria pertaining to the consequences [of the event i.,e., type of processing operation]"[1123]:

1) The potential harm for natural persons resulting from the personal data processing (e.g., discrimination, identity theft or fraud, financial loss, damage to reputation, loss of

[1117] As the words 'in particular' of Art. 35(3) indicate.

[1118] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679', vol WP 248 rev (2017) 8 <https://ec.europa.eu/newsroom/article29/items/611236/en>.

[1119] Following the line of reasoning of Art. 35(1) GDPR.

[1120] Art. 35(5) GDPR.

[1121] Art. 35(10) GDPR.

[1122] Mantelero, 'Comment to Articles 35 and 36' (n 1104) 9.

[1123] Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (n 1002) 286.

confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage);

2) The deprivation of data subjects' rights and freedoms or control over their personal data;
3) The nature of the data that has been processed (sensitive data);
4) The creation or use of personal profiles;
5) The particular conditions of vulnerable data subject, in particular of children;
6) The scale of the personal data processing (involving a large amount of personal data with an impact on a large number of data subjects).

A key challenge of every DPIA is deciding which risks and harms to individuals to consider, how to weight them and how to assess their likelihood and severity. From a first reading of Recital 75, harms to individuals might be framed in two broad categories[1124]: i) material harms (i.e., physical threat or injury, financial or economic loss, unlawful discrimination, identity theft, loss of confidentiality, accidental/unlawful destruction, alteration, unauthorised disclosure or access, unauthorised reversal of pseudonymisation, breach of professional secrecy and other significant economic or social disadvantage); ii) non-material harms (i.e., damage to reputation or goodwill, individuals deprived of rights and freedoms, or prevented from exercising control over their data).

However, Article 29 WP has made it explicitly clear that "the risks-based approach goes beyond a narrow 'harm-based-approach' that concentrates only on damage and should take into consideration every potential as well as actual adverse effect, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g., loss of social trust)"[1125]. Therefore, to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, Article 29 WP put forward nine criteria in its 2017 guidelines:

i) evaluation or scoring, including profiling and predicting;
ii) automated decision-making with legal or similar significant effect;
iii) systematic monitoring;
iv) sensitive data or data of a highly personal nature;
v) data processed on a large scale;
vi) matching or combining datasets;
vii) data concerning vulnerable data subjects;

[1124] The Centre for Information Policy Leadership, 'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR' (2016) 16 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf>.

[1125] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (2014) 4 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>.

viii) innovative use or application of new technological or organisational solutions;

ix) when the processing in itself "prevents data subjects from exercising a right or using a service or a contract"[1126].

In light of the above, the GDPR contains a non-exhaustive list of elements that a DPIA must nonetheless contain. These are: i) a systematic description of the processing and its purposes; ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; iii) an assessment of the risks to individuals' rights and freedoms; iv) the measures envisaged to mitigate the risks[1127]. If the technical and organisational measures *per* Art. 35(7)(d) GDPR cannot adequately mitigate the high risk, then the controller shall consult the competent supervisory authority prior to processing[1128], providing *inter alia* the full DPIA[1129]. The guidelines of the Working Party clarified that 'prior consultation' with the DPA must occur where "the identified risks cannot be sufficiently addressed by the data controller (i.e., the residual risks remain high) that the data controller must consult the supervisory authority"[1130].

Importantly, as the risk management process is not a 'static' assessment, DPIAs should not be seen as a one-time task[1131]. Hence, DPIAs should be periodically reviewed and re-assessed "whenever circumstances arise that significantly affect the severity and likelihood of risks or introduce new ones"[1132]. The Article 29 WP guidelines do not mention definite time periods; the choice is left up to the controller as part of its general accountability obligations[1133].

Lastly, Art. 35(9) states that, during the DPIA, controllers shall seek the views of data subjects (or their representatives, such as associations) on the intended processing, without prejudice to trade secrets, commercially sensitive information or the security of processing operations. Article 29 WP considers that those views could be gathered through several means, depending on the context (e.g., surveys, questionnaires, etc.) but if the controller deems it not appropriate to carry out this step, it is free to do so as long as it documents its justification (consistently with the accountability principle).

[1126] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 1118) 9–11.

[1127] Art. 35(7) GDPR.

[1128] Art. 36(1); recital 84 GDPR.

[1129] Art. 36(3) GDPR.

[1130] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 1118) 18.

[1131] Kosta, 'Article 35 Data Protection Impact Assessment' (n 1111) 675.

[1132] Mantelero (n 1036) 18; Art. 35(11) GDPR.

[1133] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 1118) 14.

Albeit the GDPR does not require the DPIA to be published, the Article 29 WP notes how publicity may foster consumers trust and demonstrate controllers' accountability and transparency[1134].

In the context of IoT, a preliminary reflection should revolve around the question of whether IoT data processing always require a DPIA. Thus, the Working Party mentions IoT only once, in its 8th criterion: "Internet of Things applications could have a significant impact one individuals' daily lives and privacy; and, therefore, require a DPIA"[1135]. It falls short however of a more in-depth substantiation of the extent to which a given IoT system is likely to pose a high risk and to which rights and freedoms. Against this backdrop, the Spanish DPA (AEPD) elaborates on the main IoT risks to privacy and data protection by building on the previous Article 29 Working Party Opinion on IoT (see Chapter 4)[1136]. All in all, the AEPD adds little to the six-year-prior analysis of the A29 Working Party and, more importantly, has missed the opportunity to clarify the 'risks to rights and freedoms' standard of GDPR in the IoT domain to the detriment of controllers who lack the necessary guidance to integrate a rights-based approach into DPIA methodologies.

Although not required by the GDPR, the manufacturers of IoT products or implementing applications may also carry out a DPIA. This exercise may prove to be particularly useful wherever a technological solution is likely to be used by different controllers deploying the products or applications: "of course, the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate"[1137]. As noted by Kosta, "the product provider's DPIA and sharing of information occur at the provider's discretion, unless the provider is a controller or is a processor subject to contractual obligations pursuant to Article 28(3)(f) GDPR"[1138].

[1134] ibid 18; Tamò-Larrieux (n 910) 188–189.

[1135] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 1118) 10.

[1136] AEPD, 'IoT (I): What Is IoT and Which Risks Does It Entail' (2020) <https://www.aepd.es/en/prensa-y-comunicacion/blog/iot- and-which-risks-does-it-entail>. These risks are: i) the invasive disclosure of profiles and behaviour patterns, potentially leading to surveillance; ii) lack of control and information asymmetry, potentially impeding data subjects to correctly exercise their data protection rights; iii) lack of transparency, linked to the fact that certain classic methods for obtaining consent are not easily applicable for some types IoT devices, may, in fact, render impossible to obtain valid consent or seriously affect the validity of other legal grounds; iv) the capture of personal or sensitive data of individuals which may find themselves nearby some IoT system, even if they have no intention or idea of interacting with it; v) asymmetries in the compliance level of each actor, as multiple parties participate in a IoT system with different degrees of responsibility (controllership, joint-controllership or in the role of data processor); vi) lack of appropriate security measures at any layer level, either due to the limitations of the devices themselves, or for deficiencies in the application of data protection principles from design (e.g., non-encrypted communications, passwords by defect, etc.); vii) limitations to the possibilities to remain anonymous as soon as this service is used, not to mention the risk of re-identification.

[1137] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 1118) 8.

[1138] Kosta, 'Article 35 Data Protection Impact Assessment' (n 1111) 672–673.

Before looking at the core of the 'risk to rights' requirement of Art. 35 (section 5.1.3) – which will serve as a basis for the critical analysis of existing IoT DPIA methodologies, the next section focusses on specific risk management standards to enlighten both similarities to and differences from the GDPR risk management model enshrined in Art. 35.

5.1.2 Information security risk management frameworks

The GDPR does not rely on any specific standards, nor does it adopt a detailed risk management method to comply with the risk management duty of Art. 35. Mantelero rightly observes that this approach deserves credit. "First, standardisation processes are often opaque, not open to broad stakeholder participation and influenced by the power of the industrial entities involved. Second, existing information management standards are mainly focused on security, underestimating the other aspects of the impact of data use"[1139]. In particular, this section aims to cast light on the latter aspect, that is, the rationale, value and scope underpinning international information security risk management standards to enlighten the main differences with the GDPR 'risk-to-rights' approach. To this end, the analysis briefly charts out the main characteristics of known and widely adopted methodologies, such as relevant ISO technical standards[1140].

Information security and EU data protection law i.e., the GDPR, have different rationales, although they do share some objectives. As said in Chapter 2, information security traditionally has the goal of protecting information, through the implementation of an applicable set of controls, selected through the chosen risk management process, with a focus on the organisation[1141]. Thus, the information security risk is associated with the eventuality of threats exploiting the vulnerabilities of an information asset, thereby causing harm to an organisation[1142]. The well-known CIA triad (confidentiality, integrity and availability), which had long been central to the field of computer security, has been further expanded to include other principles such as non-repudiation, authenticity, accountability and auditability[1143]. Conversely, the risk management process introduced by the GDPR

[1139] Mantelero, 'Comment to Articles 35 and 36' (n 1104) 11.

[1140] For a general overview on ISO governance and functioning, see: Peter Hatto, 'Standards and Standardization Handbook' (2010) <http://www.nanostair.eu-vri.eu/filehandler.ashx?file=12450>.

[1141] ISO/IEC 27000:2018, 12.

[1142] Although the ubiquitous IoT interconnection renders the metaphor of a 'security perimeter' rather anachronistic, it can still prove to be useful in highlighting the key concepts of information security. The vulnerability (at the design, implementation, operation or management level) can be conceived as a weakness of one or more segments of the perimeter that can leave the allegedly protected system exposed to an attack. On the other hand, a 'threat' is represented by an accidental or deliberate action, which can lead to the violation of defined security objectives.

[1143] Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri, 'An Introduction to Information Security' (2017) NIST Special Publication 800-12.

is a tool for managing risks to the rights of the data subjects, and thus takes their perspective (see sections 5.1.1 and 5.1.3)[1144].

Before delving into information security risk management standards, a classificatory remark is due, that ISO's broad body of standards has its own semantic and conceptual background. Legal and technical scholarships do not always address the intertwined concepts of risk management, risk analysis and risk assessment with the same hierarchy in mind. For example, Gellert affirms that "risk analysis is composed of two steps: risk assessment and risk management. Risk assessment measures the level of risk (in terms of likelihood and severity), while the point of risk management is to decide whether or not to take the risk"[1145]. On the other hand, ISO 31000 standard charts out the complex relationship between these concepts starting from an overarching understanding of risk management being the "coordinated activities to direct and control an organisation with regard to risk"[1146], involving "the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk"[1147]. Instead, risk assessment is defined as "the overall process of risk identification, risk analysis and risk evaluation: [it] should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders" [1148]. Finally, the goal of risk analysis is to develop an understanding of the nature, the characteristics and level of risk: "[it] provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. […] Risk analysis should consider factors such as: the likelihood of events and consequences; the nature and magnitude of consequences; complexity and connectivity; time-related factors and volatility; the effectiveness of existing controls; sensitivity and confidence levels."[1149]. Therefore, in the view of the International Standardisation Organisation, risk analysis is a step within the broader risk assessment which, in turn, is a component of the risk management process. With regard to the aforementioned concepts, this work will rely on the ISO classification.

[1144] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 1118) 17.

[1145] Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (n 1002) 280.

[1146] ISO 31000:2018, 1.

[1147] ibid 8.

[1148] ibid 11.

[1149] ibid 12.

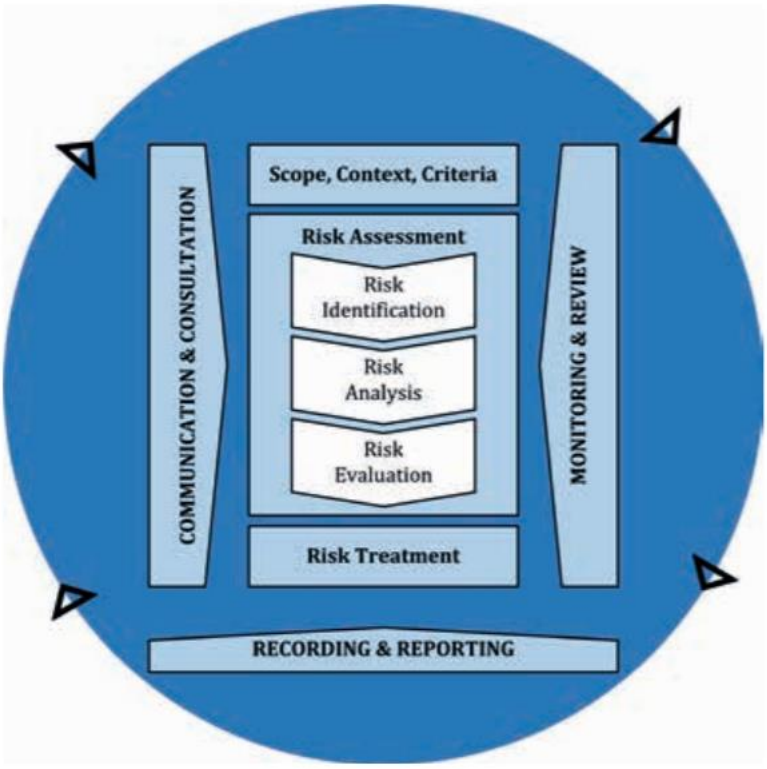


Figure 9: the interplay of risk management, assessment and analysis in ISO[1150]

The ISO 27xxx group of standards is intended to help organisations in keeping information assets secure. The best-known standard of the ISO 27xxx series is the ISO/IEC 27001, the information security management system (ISMS). It has been designed to provide requirements for implementing information security principles by following a risk management approach. Although the Plan–Do–Check–Act model (P-D-C-A)[1151] of ISO/IEC 27000 is no longer mandated by the 2017 version of the ISO/IEC 27001 standard, the well-recognised PDCA cycle still proves to be valid and effective[1152].

The 'plan' phase deals with issues like defining the scope of the ISMS, defining the roles within the organisation and how the ISMS will be managed. This part includes the definition of the risk assessment approach to identify and evaluate information security risks[1153]; the evaluation of the

[1150] ibid 9.

[1151] Aurelia Tamò-Larrieux, *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things* (Springer 2018) 173: "developers and engineers should continually improve and optimize systems by planning for security, integrating security measures, checking whether said mea- sures are working according to the plan, and acting if necessary".

[1152] Steve G Watkins, *An Introduction to Information Security and ISO27001:2013, A Pocket Guide* (Second, IT Governance Publishing 2013) 21.

[1153] The value of each asset is estimated according to the three information security attributes (i.e., confidentiality, integrity and availability) and assessed via the traditional "risk = likelihood X impact" relationship. Every organization sets its own risk-acceptance threshold, above which a decision has to be taken as to what to do about each of them (e.g., controls, accepting the risk, transferring the risk to via insurance, etc).

various options for risk treatment; the selection of the controls to be implemented for each risk[1154]; the drafting of a statement of applicability (SoA) and a risk treatment plan. The 'do' phase concerns the implementation of the planned procedures for the risk treatment plan and technical controls. The 'check' step instead consists of monitoring, reviewing, testing and auditing. Finally, the 'act' phase refers to the process of ongoing review, further testing and improvement implementation, if necessary[1155].

With the GDPR progressively setting a gold standard in data protection across the world[1156], ISO seized the opportunity to enter the EU privacy standards market, with ISO/IEC 27701 and ISO/IEC 29134 as the two prominent examples. Whereas the former is an extension of ISO 27001 providing for GDPR compliance support, the latter has been designed as a means for companies to demonstrate compliance with the obligation to conduct a DPIA.

In particular, the standard ISO 27701:2019 has been designed to enhance the ISMS contained in ISO/IEC 27001:2013 to set up a 'Privacy Information Management System' (PIMS) – an ISMS dedicated to personal data protection – to be GDPR compliant. In other words, the ISMS requirements of ISO/IEC 27001:2013 would, as an additional step, address the "protection of privacy as potentially affected by the processing of Personal Identifiable Information"[1157].

On the other hand, the ISO/IEC 29134 standard gives guidelines on how to undertake a privacy impact assessment (PIA). Notably, ISO acknowledges the PIA as part of organisations' overall information security risk management (ISMS) effort[1158]. The standard frames the PIA process in 5 subsequential steps: i) identification of the information flow, as regards personal data (personal identifiable information "PII", according to the ISO methodology); ii) analysis of the use-case's implications; iii) determination of the relevant privacy safeguarding requirements; iv) assessment of the privacy risks;

[1154] ISO lists 114 different controls within 14 categories; the list is nonetheless non-exclusive, as specific sector requirements could go beyond the generic ones. Watkins (n 50) 32 groups these controls under six categories: i) information security organisation, structure and human resources (organisation's commitment, security roles and objectives relating to information security); ii) assets, access control and classification (assets are classified to a defined labelling scheme, and the classification will indicate the level of protection required); iii) physical access and environmental issues (perimeters around secure areas should be defined in all three dimensions); iv) networks and IT (capacity planning, new developments testing, back-ups and so on); v) incidents (the need to regularly test the business continuity plans in order to learn from the experience and improve the plans ahead of any security breach); vi) compliance and internal audit (legal compliance).

[1155] Alan Clader, *Nine Steps to Success: An ISO27001:2013 Implementation Overview* (Second, IT Governance Publishing 2013) 45–46.

[1156] Jan Philipp Albrecht, 'How the GDPR Will Change the World' (2016) 2 European Data Protection Law Review 287; Alessandro Mantelero, 'The Future of Data Protection: Gold Standard vs. Global Standard' (2021) 40 Computer Law & Security Review 105500.

[1157] Eric Lachaud, 'ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification' (2020) 6 European Data Protection Law Review 194, 198.

[1158] ISO/IEC 29134:2020, *Information technology. Security techniques. Guidelines for privacy impact assessment* (2020), vi.

v) preparation for risks' mitigation. The risk is evaluated by the organisations performing the PIA by determining both the likelihood and the impact, either adopting a qualitative, semi-quantitative or quantitative method, or a combination of these, depending on the circumstances" [1159].

A twofold, conceptual and structural, misalignment between the ISO and the GDPR frameworks can already be appreciated, even after the above brief introduction of the standards under scrutiny.

From a conceptual standpoint, the approach undertook by ISO standards is inevitably narrower than the broader breadth of the GDPR. Firstly, the ISO framework is rooted in information security and thereby promotes a hierarchy that subordinates data protection to information security[1160]: whereas ISO puts information security on top of the value chain, the GDPR, as it has already been said in this work, in Art. 5(1) conceives information security or, more precisely, integrity and confidentiality[1161], as one of several other principles providing the basis for the protection of personal data[1162].

As already stressed in Chapter 2, when laying down the theoretical framework underpinning the '*infraethical* perspective', in the light of the GDPR, information security is crucial to safeguarding fundamental rights (notably, Articles 7 and 8 of the Charter) and liberties of natural persons, without being a fundamental right in itself[1163]. On the other hand, ISO recognises the protection of privacy (including, selected aspects of EU data protection) as an additional requirement to information security.

This rationale is nonetheless difficult to reconcile with the broader approach adopted by the European legislator in the GDPR, aimed at protecting "*fundamental rights and freedoms* of natural persons and in particular their right to the protection of personal data [emphasis added]"[1164], not only privacy. This is all the more true in the case of the 'risk-to-rights' standard of the data protection impact assessment of Art. 35, as addressed in the previous section. Conversely, the ISO standard for conducting a PIA details the losses of confidentiality, integrity and availability as the first factors to be weighed when assessing privacy risks. Yet, in the attempt to somewhat bridge the gap with the GDPR's approach, the standard details other aspects that ought to be considered in the privacy risk assessment, such as the "insufficient information concerning the purpose for processing the PII [personally identifiable

---

[1159] Id., 18.

[1160] Lachaud (n 1157) 204.

[1161] Art. 5(1)(f) GDPR: "including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

[1162] Cécile De Terwangne, 'Article 5. Principles Relating to Processing of Personal Data' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press 2020).

[1163] Vagelis Papakonstantinou, 'Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?' (2022) 44 Computer Law and Security Review.

[1164] Art. 1(2) GDPR.

information] (lack of transparency)", the unjustified retention of PII, or the failure "to consider the rights of the PII principal (loss of the right of access)"[1165]. Moreover, the standard explicitly suggests that organisations "examine separately privacy risks from a PII principal's point of view and privacy risks from the organisation's point of view"[1166].

The latter point leads us to a second consideration pertaining to the conceptual misalignment, that is, the perspective from which the impact assessment is carried out or, in other words, the interests to be safeguarded. Whereas ISO's ISMS and – to a large extent, also the PIA – is mainly preoccupied with the organisation, the GDPR takes the view of the data subjects, rather than the controllers[1167]. This is justified by ISO's solid anchoring to information security: ISO is "[s]tepping slightly out its comfort zone when trying to address fundamental rights issues while continuing to use essentially its old toolbox"[1168].

A further discrepancy between the two frameworks is represented by the differing terminology. As seen above, ISO privacy standards refer to 'personally identifiable information' (PII) instead of personal data; the 'PII principal' instead of data subject; 'privacy controls' instead of technical and organisational measures; and, of course, privacy to encompass data protection. This conceptual divergence may eventually create confusion for data controllers using ISO's privacy standards with the view of complying with the GDPR[1169].

With regards to the structural misalignments between the ISO and GDPR, the root of all problems is the ISO's attempt to *quantify* risks to privacy, provided that as a general rule – in data protection – "neither the severity of damage nor the likelihood of its occurrence can be meaningfully quantified"[1170]. Christofi et al. clearly explain this:

> "One may be able to quantify a system's vulnerabilities, the likelihood of external attacks and certain consequences of a data breach, e.g. as regards the number of individuals affected and the sensitivity of the personal information at stake. It is much more difficult – if not impossible – to quantify potential harms on 'rights and freedoms', which are of course intangible. Moreover, in the pursue of

[1165] ISO/IEC 29134:2020 (n 57) 16.

[1166] ibid 8.

[1167] Christofi and others (n 1112) 12.

[1168] ibid 17.

[1169] Lachaud (n 1157) 202.

[1170] Michael Friedewald and others, 'Data Protection Impact Assessments in Practice: Experiences from Case Studies', *ESORICS 2021: Computer Security. ESORICS 2021 International Workshops*, vol 13106 LNCS (Springer International Publishing 2022) 432.

quantification, ISO's approach (strictly) focuses on possible consequences for the individual data subjects, lacking a collective dimension"[1171].

In this respect, the next section will shed light on possible avenues for quantifying risk thresholds in DPIAs.

Furthermore, the risk assessment in GDPR goes beyond the ISO's narrower 'harm-based' approach. As clarified by the Article 29 WP, "risk-based approach goes beyond a narrow "harm-based-approach" that concentrates only on damage and should take into consideration every potential as well as actual adverse effect, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust)"[1172]. Indeed, the potential harms that a DPIA should be preoccupied with are not limited to ISO privacy-related risks (e.g. illegitimate use of personal information, data security), "but also include other prejudices, mainly concerning discriminatory or invasive forms of data processing"[1173].

On the other hand, it should be acknowledged that ISO 29134, when articulating the harms to users, refers to "physical, financial, reputational harm, embarrassment and invasion of domestic life [and, further,] different types of privacy such as bodily privacy, location and space privacy, behavioural privacy, privacy of communications, privacy of data and image, privacy of thoughts and feelings and privacy of associations"[1174]. As noted by Christofi et al., this list of harms, while focusing solely on privacy, rather broadens the scope of privacy ('privacy of thoughts and feelings and privacy of associations') "to the instrumental role that privacy plays with respect to other rights and freedoms of individuals"[1175]. Such phrasing can arguably be seen as yet another attempt of ISO to fill the gap with the broad fundamental rights perspective of the GDPR.

Yet, companies as data controllers that have to operationalise the high-level 'risk-to-fundamental-rights' legal standard set by the GDPR, find it easier to "articulate a number of more measurable 'harms' concerning data security breaches"[1176]. To make things more complex, Annex 2 of the Guidelines of Article 29 WP Guidelines on DPIA lays down the criteria that data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR. However, when it comes to the assessment of the risks to the rights and

---

[1171] Christofi and others (n 1112) 14.

[1172] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (n 1125) 4.

[1173] Mantelero, 'Comment to Articles 35 and 36' (n 1104) 21.

[1174] ISO/IEC 29134, Clause 6.3.1.

[1175] Christofi and others (n 1112) 13.

[1176] Quelle (n 1108) 505–506.

freedoms of data subjects (step 3), the Guidelines unduly restrict the scope on data security[1177], not only with regard to the events leading to the risk[1178] but also with regard to the risks itself: "origin, nature, particularity and severity of the risks are appreciated (cf. Recital 84) or, more specifically, for each risk (*illegitimate access, undesired modification, and disappearance of data*) from the perspective of the data subjects [emphasis added]"[1179]. This is confusing at best.

Moreover, in Annex 1 the Guidelines explicitly call on ISO/IEC 29134 as an "international standard [that] will provide guidelines for methodologies used for carrying out a DPIA". Without dwelling on the delicate and critical issue of delegation of regulatory power to a private body[1180], against the background of the misalignment of ISO 29134 with the GDPR's 'risk-to-fundamental-rights' approach Christofi et al note that there is no evidence that Article 29 WP performed a due diligent assessment with the endorsement of the ISO standard amounting to a 'blank cheque'[1181].

All in all, "ISO/IEC 29134 should be designed and used for what it can really provide rather than be subtly re-branded as a DPIA methodology"[1182]. The value of ISO international standards such as ISO 27701 and ISO 29134 lies in showing how compliance to requirements and controls of ISO/IEC standards can be relevant to fulfilling the obligations of GDPR. For example, the informative Annex D of ISO 27701 outlines an indicative map between the provisions of the standard and Articles 5-49 of the GDPR (except for Article 43)[1183]. These data protection requirements regard, *inter alia*: management of personal data breach; identification of a legal basis for processing personal data (specifying how to obtain and record consent); privacy (data protection) impact assessment;

[1177] ibid 506.

[1178] Article 29 Data Protection Working Party (n 16) 22: "potential impacts to the rights and freedoms of data subjects are identified in case of events including *illegitimate access, undesired modification and disappearance of data*" [emphasis added].

[1179] ibid.

[1180] This is part of a broader problem concerning the position of EU authorities on the legal status of standards (see CJEU C-613/14 James Elliott Construction ECLI:EU:C:2016:821). In turn, this generates problems in data protection law (as seen, uptake of ISO based DPIA could weaken the level of protection offered by the GDPR), competition law (the use of conformity assessment processes may conflict with EU competition law when they contribute to exclude competitors from the market and/or when they distort the conditions of access to the market at the expenses of certain competitors, see Victoria I Daskalova and Michiel A Heldeweg, 'Challenges for Responsible Certification in Institutional Context: The Case of Competition Law Enforcement in Markets with Certification' in Peter Rott (ed), *Certification – Trust, Accountability, Liability* (Springer Cham 2019) and constitutional law (see Marie Gérardy, 'Nemo Censetur Ignorare Legem: The Dilemma Regarding the Access to ISO Standards Referenced into EU Law' (*REALaw.blog*) <https://realaw.blog/2021/11/23/nemo-censetur-ignorare-lege-the-dilemma-regarding-the-access-to-iso-standards-referenced-into-eu-law-by-marie-gerardy/> accessed 7 December 2021).

[1181] Christofi and others (n 1112) 18.

[1182] ibid 17.

[1183] ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*, 67.

relationship with data processors; joint controllership; obligations to data subjects (herein called PII principals) and privacy by design and by default[1184].

On the other hand, data protection supervisory authorities have not yet provided controllers with the proper guidance on how to operationalise the challenging rights-based approach at the core of the DPIA into methodologies. While sections 5.2.1 and 5.2.2 will investigate a specific DPIA methodology (for IoT devices) developed by the French DPA more closely, the next section further investigates paths for meaningfully substantiating the GDPR's 'risk-to-fundamental-rights' standard into DPIA methodologies.

On a last note, it should be noted that ISO/IEC are working to establish IoT *cybersecurity&privacy* guidance. The international standard (ISO/IEC) 27402, *Cybersecurity — IoT security and privacy — Device baseline requirements* is currently under development: the proposal was approved in mid-June 2020[1185].

5.1.3 Towards a holistic, fundamental rights-based DPIA

In light of the above, this section aims to provide a theoretical framework for meaningfully integrating a comprehensive fundamental rights assessment in a generic, that is, not sector- or case-specific, DPIA model in order to provide useful benchmarks for a DPIA designed specifically for IoT devices later addressed in the following sections.

The concept of 'rights and freedoms' in Art. 35(7)(c) should be read as a reference to *all* fundamental rights and freedoms, as convincingly put by Hallinan and Martin. Among the three arguments made by the authors to substantiate their thesis[1186], the most significant is perhaps considering the DPIA risk assessment process in light of the overarching goal of the GDPR enshrined in Article 1(2), stating the Regulation's objective, that is, to protect 'the *fundamental rights and freedoms of natural persons* and in particular their right to the protection of personal data [emphasis added]'[1187]. "In this statement, there is no indication that the concept of fundamental rights and freedoms should be understood to deviate from the [full catalogue of EU fundamental rights framework]"[1188]. Indeed, Article 29 WP

[1184] ibid 33-51.

[1185] See https://www.iso.org/standard/80136.html

[1186] These are: i) a consideration of the DPIA risk assessment process in light of other substantive provisions in the GDPR, such as the fairness principle (Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130); and, ii) a consideration of the DPIA risk assessment process in light of the phenomena it seeks to regulate.

[1187] Durante (n 20) 130: "Art. 1(2) GDPR conveys a conception of law as a means to affirm and protect a human person in some fundamental respect, that is, with regard to what is situated at the foundation of the construction of personality".

[1188] Hallinan and Martin (n 1116) 183. Hallinan and Martin convincingly contend that the European fundamental rights framework can fulfil the criteria they previously identified for a legitimate normative reference point in (data protection) risk assessment. Thus, EU fundamental rights framework i) represents a normatively ideal state of being; ii) has a

points out in the DPIA Guidelines that "the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion"[1189]. However, as noted in the previous section, the examples of risks made by the Guidelines solely focuses on information security.

If the attention is devoted to DPIA models currently made available by supervisory authorities, to provide guidance to data controllers, then it can be observed that generally the risk assessment phase does not encompass the full breadth of Art. 35(7)(c). Thus, the traditional European data protection's procedural approach has led DPA to design risk assessment models (PIA, i.e. Privacy Impact Assessment, under the Data Protection Directive) that are primarily centred on the processing, task allocation, data quality, and data security, leaving aside the nature of safeguarded interests: "despite specific references in the GDPR to the safeguarding of rights and freedoms in general as well as to societal issues, the new assessment models do nothing to pay greater attention to the societal consequences than the existing PIAs"[1190].

For example, Friedewald et al. evaluate and compare DPIA methods from various authorities (i.e., French, British, German and Dutch) to design and test a DPIA process generic enough to be used in all possible application areas[1191]. However, in the DPIA execution phase, and more specifically in the risk identification step, they identify solely 'privacy risks' – although they previously acknowledged that the focus of the execution phase should be on the assessment of risks to the rights and freedoms of data subjects pursuant to Art. 35 (7)(c) GDPR[1192].

Against this background, after having examined the Article 29 WP guidelines for a DPIA in the previous section, the ENISA methodology may provide useful insights on the extent to which the guidance from EU authorities, notably the EU cybersecurity agency, holistically considers rights and freedoms without flattening the assessment to a pure information security risk-management approach.

---

relationship with the phenomenon (i.e., the processing of personal data) which poses the harm to be evaluated in the risk assessment process; iii) the nature and likelihood of impacts is uncertain from the outset, that is, in between neither known nor unknowable.

[1189] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 1118) 6.

[1190] Alessandro Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (Springer 2022) 23. The author rightly points out that "whereas the driving values behind data security and data management are technology-based (e.g. integrity of data) and can therefore be generalised across varying social contexts, the situation with regard to social and ethical values is different. These are necessarily context-based and differ from one community to another, making it hard to pinpoint the benchmark to adopt for this kind of risk assessment". Cfr. with Tamò-Larrieux (n 847) 189: the author highlights that the alingment of DPIA models towards risk management shifts the focus from transparency to security when considering the technical mechanisms for data protection.

[1191] Friedewald and others (n 1170).

[1192] ibid 430.

In its report 'Handbook on Security of Personal Data Processing', ENISA presents an evaluation of risk approach that can be deployed "in all cases where risk assessment is envisaged under the Regulation (e.g. Data Protection Impact Assessment)"[1193]. It has four consequential steps: i) definition of the processing operation and its context; ii) understanding and evaluating impact; iii) definition of possible threats and evaluation of their likelihood; iv) evaluation of risk.

The first step aims to define the processing operations and its context. For the purpose of this work, it is worth dwelling more extensively on the second step, that is, understanding and evaluation of the impact. Importantly, ENISA clarifies from the outset that at this stage the data controller must specifically assess "the impact on the fundamental rights and freedoms of the individuals, resulting from the possible loss of security [i.e., confidentiality, integrity and availability] of the personal data"[1194]. Moreover, the handbook provides a short but effective informative description of examples for each of the four levels of impact considered (low, medium, high, very high). The impacts on the 'rights and freedoms of natural persons' span from minor (such as time spent re-entering information, irritations) and significant (e.g., extra costs, denial of access to business services, fear, lack of understanding, stress) inconveniences to significant (e.g., misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment) or irreversible (inability to work, long-term psychological or physical ailments, death) consequences[1195]. It is clear therefore that the risks contemplated by ENISA does not pertain solely to 'privacy' or information security but rather they encompass a much broader set of rights and freedoms. Moreover, ENISA also acknowledges that risk assessment is a qualitative process, as a quantitative analysis is not well suited[1196], and a number of factors must be considered by the data controller. Consistently, in the online tool for the security of personal data processing, the EU cybersecurity agency maintains the distinction between security risk assessment and DPIA: "while the former is a critical part of the latter, a DPIA takes into account several other parameters that are related to the processing of personal data and go beyond security"[1197].

The third step defines the possible threats related to the *overall* processing's environment and assesses their likelihood (threat occurrence probability), whereas the fourth step consists of the final evaluation of risk, according to the evaluation of likelihood and impact.

[1193] ENISA, 'Handbook on Security of Personal Data Processing' (2017) 6 <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing>.

[1194] ibid 10.

[1195] ibid 11.

[1196] The Danish Institute for Human Rights, 'Human Rights Impact Assessment: Guidance and Toolbox' (2020) 98 <https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/udgivelser/hria_toolbox_2020/eng/dihr_hria_guidance_and_toolbox_2020_eng.pdf>; Friedewald and others (n 1170) 432.

[1197] https://www.enisa.europa.eu/risk-level-tool

Future data protection impact assessment models, especially in data-intensive systems such as the IoT, should be broader in scope so that the full catalogue of EU fundamental rights and freedoms is appropriately contextualised and assessed in the specific use case scenario. A sector-specific approach shall focus on the rights and values potentially impacted in the case under scrutiny rather than the technology itself (AI, IoT, etc.). Depending on the application domain (see Chapter 1; e.g., domotics, healthcare, industry, etc.), different sets of rights, freedoms and values are at stake. It follows that sectoral (that is, not generic) assessment models should be concerned with the context and the values that assume relevance in a given context.

Bearing this in mind, the second part of this Chapter hinges on a DPIA model for the IoT. In particular, it aims to provide a structured methodology which would effectively and comprehensively realise the requirement of Art. 35 to assess the risks to rights and freedoms arising in IoT environments, by building on the CNIL DPIA methodology for IoT devices. In doing so, it will seek to be general rather than sector specific. On the other hand, it is worth remembering that the DPIA model analysed and proposed in the next sections is not a technological assessment but a methodology that should assist sector-specific IoT DPIA in conducting rights-based and values-oriented assessments.

5.2 Holistic Risk Analysis Methodology for IoT

5.2.1 The CNIL DPIA methodology for IoT devices

This section presents the methodology developed by the French Data Protection Authority (CNIL), which first published– among the others DPAs –guidelines for conducting a DPIA in the specific context of IoT devices back in 2018, taking as an example a fictional generic interactive toy, a mobile app and an online service[1198].

The model is based upon the CNIL's DPIA methodology which, in turn, is made up of three guides, publicly accessible from the agency website: the PIA methodology[1199]; the PIA templates[1200]; and the PIA knowledge bases[1201]. The first charts out the approach, the second contains elements that could be used in formalising the analysis and the third one provides a knowledge base, or rather a catalogue of controls to comply with legal requirements and to manage risks, with examples.

[1198] CNIL, 'PIA: Application to IoT Devices' (2018) <https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual> accessed 31 January 2020.

[1199] CNIL, 'Privacy Impact Assessment (PIA) Methodology' (2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf>.

[1200] CNIL, 'Privacy Impact Assessment (PIA) Templates' (2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf>.

[1201] CNIL, 'Privacy Impact Assessment (PIA) Knowledge Bases' (2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>.

The model consists of four phases: i) study of the context; ii) study of the fundamental principles; iii) study of data security risks; iv) validation of the DPIA. Importantly, the CNIL (D)PIA methodology guidelines state that the CNIL model covers all the criteria of the WP29 guidelines[1202] i.e., i) a systematic description of the processing (Art. 35(7)(a) GDPR); ii) assessment of necessity and proportionality (Art. 35(7)(b) GDPR); iii) management of risks to the rights and freedoms of data subjects (Art. 35(7)(c) GDPR); iv) involvement of the interested parties (Art. 35(7)(c) GDPR)[1203].

The first phase of the DPIA aims to provide a clear overview of the personal data processing operations. Firstly, the model suggests presenting the IoT device scrutinised (a connected toy, in the CNIL example), its nature, scope, context, purposes and stakes. In terms of the data processing, the preliminary step is to identify the data controller and processors, if any. Afterward, sector-specific (either voluntary or mandatory) standards applicable to the processing at stake must be listed, including the approved codes of conduct (art. 40 GDPR) and certifications (art. 42 GDPR). Processing can then be defined and described in detail. The data controller has to take into account three different layers of complexity. They regard: i) the data processed (which categories of personal data are involved; who the recipients are; the persons with access thereto; the duration of the storage); ii) the life cycle of data processing (how the product works, with a diagram of data flows and a description of the processes carried out); iii) data supporting assets (IT systems on which the data rely and other supporting assets).

The second phase of the DPIA interestingly targets manufacturers of IoT devices first of all. Thus, the core objective of this step is to "build the system that ensures compliance with privacy principles"[1204]. Behind this lies a presumption that the manufacturer is usually the data controller of the IoT data processing. In particular, the CNIL suggests explaining and justifying the technical choices and the controls selected in the design phase vis-à-vis compliance with GDPR fundamental principles and legal requirements. This analysis comprises two progressive assessments: i) assessment of the controls guaranteeing the proportionality and necessity of the processing; ii) assessment of controls protecting data subjects' rights.

The former breaks down the processing operations with a view to checking compliance with the GDPR principles envisaged by Art. 5(1). In particular, the data controller shall: i) set out the purposes of the processing and justify their legitimacy[1205]; ii) identify a suitable legal basis for the processing

---

[1202] CNIL, 'Privacy Impact Assessment (PIA) Methodology' (n 1199) 11.

[1203] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 1118) 22.

[1204] CNIL, 'PIA: Application to IoT Devices' (n 1198) 6.

[1205] Art. 5(1)(b) GDPR.

to comply with the lawfulness criteria as per Art. 6 GDPR; iii) minimise the personal data that will be processed to what is strictly necessary for the purposes for which they are processed[1206]; iv) set out the data quality compliance controls[1207]; v) define a storage duration for each type of data justified by the legal requirements[1208].

The latter casts the light on the controls protecting data subjects' rights. In particular, the data controller shall: i) describe how controls for the right to information are implemented on the device, mobile app and personal account, pursuant to Articles 12, 13 and 14 GDPR[1209]; ii) demonstrate that the data subject has consented (where applicable) and provide the data subject with the possibility to easily withdraw his/her consent at any time, pursuant to Articles 7 and 8 GDPR[1210]; iii) ensure users' right of access to all personal data concerning them and to data portability, pursuant to Articles 15 and 20 GDPR[1211]; iv) ensure the rights to rectification and erasure, pursuant to Articles 16 and 17 GDPR[1212]; v) ensure the right to restriction of processing (either concerning the different purposes or the entire operation) and right to object, pursuant to Articles 18 and 21 GDPR[1213]; vi) identify any data processors in the processing contract, by detailing the contractual terms of their relationship with the data controller pursuant to Articles 28 GDPR[1214]; vii) set out the geographic storage location of the device, mobile app and personal account data in the cloud, that is, comply with the obligations concerning the transfer of personal data outside the European Union, pursuant to Articles 44 to 50 GDPR and applicable case-law[1215].

The third phase of the DPIA focuses on the risks posed to data security, with a specific reference to Article 32 GDPR. This phase is once again divided into two sequential assessments: the assessment

---

[1206] Art. 5(1)(c) GDPR.

[1207] Art. 5.1(d) GDPR.

[1208] Art. 5.1(e) GDPR.

[1209] Here, technical controls may include the easy display of terms & conditions; clauses specific to the device; thorough presentation of the personal data collected; legible presentation of the purposes of transmission to third parties, etc.

[1210] Here, technical controls may include express consent during activation, segmented consent *per* data categories, express consent prior to sharing data with other users, obtaining parents' consent for minors under 13 years of age, etc.

[1211] As regards technical controls enforcing the right of access, specific controls might include the possibility of accessing all the user's personal data, via the common interfaces or the possibility of securely consulting the traces of use associated with the user; as regards the right to data portability, the possibility of retrieving, in an easily reusable format, personal data provided by the user, so as to transfer them to another service.

[1212] Here, technical controls may include the possibility of rectifying personal data; possibility of erasing personal data; indication of the personal data that will nevertheless be stored, etc.

[1213] Here technical controls may include the existence of 'Privacy' settings; an invitation to change the default settings; possibility to access the 'Privacy' settings when activating and after activating the device; existence of a parental control system for children under 13 years of age, etc.

[1214] The aspects to be included in the agreement shall cover: duration, scope, purpose, documented processing instructions, prior authorisation where a processor is engaged, prompt notification of any data breach, etc.

[1215] The CJEU, with the seminal *Schrems II* ruling (Case C-311/18 *Facebook Irland and Schrems* [2020] EU:C:2020:559), has once again invalidated the Commission's adequacy decision (so-called Privacy Shield) on transfers of personal data to the US.

of existing or planned (security) controls and a traditional information security risk assessment bearing on potential *privacy* breaches.

The assessment of security controls, generally performed by the person in charge of data security aspects, is threefold, for it identifies: i) controls specifically aimed at the data being processed: encryption[1216], anonymisation[1217], data partitioning[1218], logical access control[1219], traceability[1220], archiving[1221], integrity monitoring and paper document security; ii) general security controls regarding the system in which the processing is carried out: operating security[1222], backups, hardware security, network security[1223], physical access control, monitoring, maintenance, website security, protecting against non-human sources of risks; iii) organisational controls (governance): organization[1224], policy, project management, personnel management, risk management[1225], management of incidents and breaches, relations with third parties, supervision.

The risk assessment then takes into account three feared events that can potentially lead to privacy breaches, all pertaining to the field of information security and, more specifically the 'CIA triad': illegitimate access (breach of personal data confidentiality); unwanted change (breach of data integrity); disappearance (breach of data availability). In accordance with classic Infosec risk assessment models, the risk level is estimated by determining its severity (i.e., the potential impact) and likelihood (i.e., the possibility of a risk occurring). In the context of the fictional IoT device, for each breach, the CNIL has considered the main risk sources, the main threats, the main potential impacts, the principal controls mitigating the risk, and the severity and likelihood.

[1216] The CNIL suggests describing the encryption means for data at rest and data in transit implemented in the processing, as well as the procedure for managing encryption keys.

[1217] The CNIL suggests indicating whether anonymisation mechanisms are implemented, which ones and for what purpose.

[1218] Whether it is planned, and how, or not.

[1219] The CNIL suggests indicating the specification of the implemented authentication means and password criteria

[1220] Whether events are logged and for how long.

[1221] The CNIL suggests describing the archiving management processes.

[1222] Description of how software updates and security patches are implemented.

[1223] Description of the type of network on which the processing is carried out and specification of which firewall system, intrusion detection systems or other active or passive devices are in charge of ensuring network security.

[1224] Whether the roles and responsibilities for data protection and cybersecurity are defined.

[1225] Whether the privacy risks posed by new processing on data subjects are assessed, whether or not it is systematic and, if applicable, according to which method.

3.2.1 Illegitimate access to personal data

Assessment of the risk

Below you will find a table for noting down the result of the analysis of this risk.

To show how to use it, it has been completed with the data from our example of a fictional toy.

Risk	Main risk sources[56]	Main threats[57]	Main potential impacts[58]	Main controls reducing the severity and likelihood[59]	Severity[60]	Likelihood[61]
Illegitimate access to personal data	Rogue acquaintances Rogue neighbor Rogue employee Authorized third-party company Hacker targeting a user or one of the companies	Data theft/consultation on the server Account theft (via a smartphone) Recovery of a scrapped device	Consequences of the disclosure of potentially sensitive information (discrimination, threats, attacks, loss of employment, loss of access to services, ***etc.***) Phishing Targeted advertising	Minimization Storage durations Logical access control Stream encryption (SSL) Hardware authentication Private cloud Logical access control Employee clearance Access logging Log audits Notification of data subject violations and recommendation of suitable preventive controls	Significant	Maximum

Figure 10: CNIL's IoT device risk assessment regarding breach of data confidentiality[1226]

3.2.2 Unwanted change of data

Assessment of the risk

Below you will find a table for noting down the result of the analysis of this risk. To show how to use it, it has been completed with the data from our example of a fictional toy.

Risks	Main risk sources	Main threats	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Unwanted change of data	Negligent or rogue user /family member /friend Rogue neighbor Negligent or rogue employee Hacker targeting one of the companies	Alteration of data on the server	Identity theft Deterioration in the service quality	Backup of the cloud server Stream encryption (SSL) Hardware authentication Private cloud Logical access control Employee clearance Access logging Log audits Notification of data subject violations and recommendation of suitable preventive controls	Limited	Limited

Figure 11: CNIL's IoT device risk assessment regarding breach of data integrity[1227]

[1226] CNIL, 'PIA: Application to IoT Devices' (n 1198) 28.

[1227] ibid 30.

3.2.3 Disappearance of data

Assessment of the risk

Below you will find a table for noting down the result of the analysis of this risk. To show how to use it, it has been completed with the data from our example of a fictional toy.

Risks	Main risk sources	Main threats	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Disappearance of data	Negligent or rogue user /family member /friend Negligent or rogue employee Hacker targeting a user or one of the companies Damage at one of the companies	Erasure of data (via the app or server) Deterioration of servers Physical damage to the device	Need to recreate a user account Loss of history and personal service settings Deterioration in the service quality	Backup of the cloud server Private cloud Physical protection of the cloud servers Maintenance Temporary on-premises data retention Logical access control Employee clearance Strong authentication of employees Access logging Warranty for the device	Limited	Limited

Figure 12: CNIL's IoT device risk assessment regarding breach of data availability[1228]

Afterwards, it is necessary to assess whether the existing or planned controls sufficiently mitigate the risk. If any additional control may prove necessary, it will be indicated. Finally, once the additional controls have been implemented, the residual risk will be determined by determining the severity and likelihood in view of such additional controls.

The last phase of the DPIA, consisting of the model's validation, is divided into two steps: preparation of the material required for validation and the formal validation. The former serves a twofold purpose: presenting the findings of the DPIA (i.e., visual presentation of the controls as *per* phase 2 and 3, mapping the risks – initial and residual, if any – depending on their severity and likelihood, drafting an action plan to implement the additional controls) and documenting the consideration of stakeholders (i.e., advice of the DPO, pursuant to Article 35(2) GDPR and the view of data subjects or their representatives, pursuant to Article 35(9) GDPR). The latter consists of deciding whether the selected controls, residual risks and action plan are acceptable, with justifications, in view of the previously identified stakes and views of the stakeholders: the DPIA can be validated, conditional on improvement or refused.

[1228] ibid 31.

5.2.2 A critical analysis of the CNIL model: consistency with the holistic 'risk-to-rights' approach

In light of the first part of the Chapter, this section provides a critical discussion regarding the CNIL DPIA methodology for IoT devices. Different layers of complexity are under scrutiny. They regard: i) whether and to which extent the methodology integrates a rights-based assessment; ii) how the methodology strikes a balance between, on the one hand, information security and, on the other, the more-encompassing concept of cybersecurity (see Chapter 2); iii) to what extent the methodology is suitable for a generalisation of the IoT domain.

5.2.2.1 The 'rights-based' test

By operationalising the DPIA as a compliance check of both GDPR and IT requirements, the CNIL methodological approach has become the most popular[1229]. Sion et al. carried out a comprehensive state-of-the-art review of existing approaches and tools to support DPIA, which range from simple template and questionnaire-based approaches to dedicated modelling frameworks[1230]. These models are taken from national Data Protection Authorities guidelines (in particular, French, German and Dutch), available commercial tools and specific literature on privacy and security requirements engineering. According to the indicators used as proxies by the authors in their analysis[1231], the CNIL approach was found to be the most complete, outscoring the German and Dutch approaches in terms of support for the evaluation of model completeness and soundness and support for identifying legal compliance issues[1232].

With specific regard to the identification of legal compliance issues, the approach adopted by CNIL has also been referred to as 'compliance assessment': "this approach suggests a DPIA risk assessment need only take the concrete principles outlined in the GDPR – such as those in Articles 5 (b)-(f), 6-8, 12-18, 20, 21, 28 and 44-49 – as a normative reference point. An assessment of risks to the concrete principles in the GDPR should certainly be included as part of the DPIA risk assessment process. However, a consideration of risks to these concrete data protection principles alone does not equate to a consideration of risks to all rights and freedoms"[1233].

This is therefore the focal point of the first legal issue raised by CNIL methodology, i.e., to what extent the DPIA methodology for IoT devices integrates an assessment of the risks to the rights and

---

[1229] Friedewald and others (n 1170) 425–426.

[1230] Laurens Sion and others, 'DPMF: A Modeling Framework for Data Protection by Design' (2020) 15 International Journal of Conceptual Modeling 1.

[1231] DPIA methodology support; coverage of A29WP concepts; support for soundness criteria; support for legal criteria; tool support; document generation and model management.

[1232] Sion and others (n 1230) 8–9.

[1233] Hallinan and Martin (n 1116) 184.

freedoms of data subjects, whereas the other criteria of the WP29 guidelines are convincingly covered by the French model. In this regard, the title of the third phase of the DPIA, i.e., the 'study of data security risks'[1234], is rather eloquent. On the one hand, the analysis of information security controls in the CNIL model, contrary to traditional security risk assessment models, is not the starting point for the effective implementation of data protection, but instead, comes after implementation of the controls on the proportionality and necessity of the processing and the controls protecting data subject's rights (see section 5.2.1)[1235]. It follows that, in the CNIL's view, information security facilitates the data protection goal of attaining the lawfulness of the processing. This approach recalls the infraethical perspective of Chapter 2, that is, a good infraethical construction of cybersecurity measures that is oriented towards facilitating the occurrence of what is morally good: the protection of personal data and the safeguarding of rights and freedoms of individuals. Using the words of the Spanish Data Protection Authority (AEPD), "the technical and organisational measures needed to ensure the confidentiality, integrity and availability of information must be aimed at implementing data protection principles to guarantee the rights and freedoms of individuals in a State governed by the rule of law, even beyond a potential breach of the rule of law"[1236].

On the other hand, by using data security risks as feared events underpinning the assessment, the CNIL DPIA is "merely a data security methodology"[1237]. More importantly, though, the second step of the third phase advises data controllers "to determine the potential impacts on data subjects' privacy", unduly restricting the scope of the DPIA to a 'privacy impact assessment'. In so doing, the CNIL methodology fails to take into consideration the full breadth of the GDPR's requirements for a DPIA, with particular regard to the obligation of assessing the 'risks to the rights and freedoms of natural persons' as per Art. 35(7)(c). IoT personal data processing may thus impact individuals in many ways, going beyond risks to privacy and data protection.

Beyond the rights and freedoms already mentioned in the Article 29 WP Guidelines (i.e., freedom of expression and information (Art. 11 of the EU Charter of Fundamental Rights), freedom of movement (Art. 45 EU Charter), freedom of thought, conscience and religion (Art. 11 EU Charter), right to

---

[1234] CNIL, 'PIA: Application to IoT Devices' (n 1198) 22.

[1235] In the phrasing of the CNIL, this subset of controls is generally carried on by the prime contractor (which can be a delegate, representative or processor) and then assessed by the person in charge of data security: i.e., the chief information security officer (CISO) or the DPO themselves. It is evident that a sort of holistic approach is already in place: the cyber or information security controls weighing specifically on the data being processed are assessed, by the CISO, in order to better understand the privacy risk. Against this background, there are attempts to integrate the CNIL DPIA with the EBIOS risk manager, the method for assessing and treating digital cybersecurity risks published by National Cybersecurity Agency of France (ANSSI).

[1236] AEPD, 'Data Protection and Security' (*Prensa y comunicación*, 2020) <https://www.aepd.es/en/prensa-y-comunicacion/blog/data-protection-and-security>.

[1237] Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (n 1002) 283.

liberty and security (Art. 6 EU Charter) and prohibition to discriminate (Art. 21 EU Charter))[1238], the negative consequences suffered by individuals brought about by IoT data processing – e.g., from fear and stress to more significant impacts such as, misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment or inability to work, long-term psychological or physical ailments and death – can be mapped out to other rights and freedoms from the EU fundamental rights framework.

The fictional connected toy analysed by the CNIL makes no exception. For example, Art. 3 of the Charter protects the integrity of a person's body, both mental and physical[1239]: interferences with this right consist of the causation of injuries, pain, or other bodily and mental harm[1240]. The IoT, being a cyber-physical intermediating system, brings about risk factors that potentially result in a range of harms which span from mental damage to physical injury[1241]. A DPIA for IoT devices, and specifically for a connected toy, should take into consideration Art. 3 of the Charter.

Given the interaction between the connected toy and young users, who can be influenced by the device's value-laden content that is either shaped by the manufacturer or – more dangerously – continuously by an embedded AI, further concerns are linked to freedom of thought (Art. 10 CFR[1242]) and the right to education, in particular, the right of parents to guarantee the education and teaching of their children in conformity with their religious, philosophical and pedagogical convictions (Art. 14 CFR[1243]).

By mirroring the logic of pre-GDPR 'PIAs', the CNIL risk assessment is more preoccupied with a technical understanding of *privacy*, in line with information security's tradition. It can be concluded that the CNIL falls short of meaningfully integrating a rights-based assessment in its DPIA methodology.

However, the GDPR requirement is not truly attained in other risk assessment models proposed for IoT systems either. For example, in order to address the constant discovery of vulnerabilities in IoT components, the ANASTACIA H2020 project developed a 'Dynamic Security and Privacy Seal',

---

[1238] Article 29 Data Protection Working Party (n 16) 6.

[1239] Conversely, the ECtHR envisages the protection of physical and mental integrity under the right to private life (Art. 8 ECHR). See ECtHR, *X and Y v the Netherlands*, CE:ECHR:1985:0326JUD000897880, para 22; ECtHR, *Stubbings and others v UK*, CE:ECHR:1996:1022JUD002208393, para 61.

[1240] Tobias Lock, 'Article 3 CFR: Right to the Integrity of the Person' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press 2019).

[1241] Denardis (n 17) 224.

[1242] Tobias Lock, 'Article 10 CFR: Freedom of Thought, Conscience and Religion' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press 2019).

[1243] Tobias Lock, 'Article 14 CFR: Right to Education' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press 2019).

combining security and privacy standards and real time monitoring and online testing. The 'Seal' aims to provide a quantitative and qualitative run-time evaluation of privacy risks and security levels, which can be easily understood and controlled by the final users[1244].

The deliverable D2.3 modelled relevant privacy risks to be addressed by ANASTACIA: the consortium identified seven risks to the rights and liberties of individuals taking place at the IoT network level. They regard: i) unauthorised access/disclosure of personal data (loss of confidentiality); ii) unauthorised modification of personal data (loss of integrity); iii) unauthorized or inappropriate linking of personal data (potential for data re-identification); iv) unauthorized removal or deletion of personal data (loss of availability); v) excessive collection or retention of personal data (loss of operational control); vi) lacking protection of traffic information and location data; vii) impairment of data subject's rights[1245].

At first sight, the ANASTACIA project managed to go beyond traditional information security risks to the CIA triad (points i), ii) and iv)). Thus, the introduction of the risk for data re-identification, loss of operational control and impairment of data subject's rights is an attempt to meaningfully quantify the GDPR requirement to assess risks to individuals' rights and freedoms. A closer look, however, reveals that the reference to the impairment of data subject's rights, which seemingly assure compliance with the challenging high standard of the GDPR, is nothing more than a void, final clause. Indeed, ANASTACIA does not specify what this risk actually amounts to, since it only addresses the underlying threats: Dos and DDoS attacks (see Chapter 1)[1246].

5.2.2.2 Adequacy of the cybersecurity risks' coverage

The second issue hinges on whether the IoT cybersecurity risk is adequately assessed by the CNIL DPIA. As stated, the third phase focuses on 'data security risks', with the feared events being illegitimate access, unwanted change and disappearance of personal data, covering the notorious 'CIA' triad (confidentiality, integrity and availability) of information security.

The question to be asked is whether in 'IoT scenarios', that is, environments with connected devices interacting with other systems and individuals, the feared events that ought to be considered by the risk assessment should not be limited to the CIA triad but rather extends to other principles of cybersecurity as seen in previous Chapters. In particular, Art. 51 of the Cybersecurity Act sets a comprehensive and high-level set of security objectives within the context of a broad and general

---

[1244] ANASTACIA Project, 'Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures ' (*2019*) <https://cordis.europa.eu/project/id/731558> accessed 29 August 2022.

[1245] Adrian Quesada Rodriguez and others, 'D2.3 ANASTACIA: Privacy Risk Modelling and Contingency Initial Report' (2018) 52–60 <www.ANASTACIA-h2020.eu> accessed 29 August 2022.

[1246] ibid 57.

notion of cybersecurity that goes beyond information security, to include device and network security. This provision can be taken as a benchmark irrespective of the fact that it was originally conceived for the purpose of certification schemes[1247]. The security objectives laid down by Art. 51 CSA are:

a. to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;

b. to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;

c. that authorised persons, programmes or machines are able only to access the data, services or functions to which their access rights refer;

d. to identify and document known dependencies and vulnerabilities;

e. to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

f. to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

g. to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;

h. to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;

i. that ICT products, ICT services and ICT processes are secure by default and by design;

j. that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

Whereas illegitimate access is covered by letter a) and c) of Art. 51, letter b) aims to avoid the unwanted change and disappearance of data. The remaining objectives can be mainly linked to security controls, already foreseen by CNIL methodology. In particular, letters e) and f) are covered by logical access control and traceability requirements under section 3.1.1 of the DPIA. Moreover,

[1247] Wavestone - CEPS - CARSA - ICF, 'Study on the Need of Cybersecurity Requirements for ICT Products - No. 2020-0715: Final Study Report' (2021) 166 <https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products>: "Art. 51 was taken as a reference as it represents one of the most up-to-date piece of legislation concerning cybersecurity and providing a comprehensive set of requirements for products and services".

letter h) and j) deal respectively with backups and updates controls that are listed in section 3.1.2 of the DPIA. If the 'security by design and by default' objective outlined in letter i) is too high-level to be considered a security control or an operationalisable objective, letters d) and g) are preoccupied with the issues of vulnerabilities.

If it is true that, on the one hand, identifying and managing systems' vulnerabilities can be considered a technical control, on the other hand, the possible exploitation of known vulnerabilities may indeed represent a feared event with a potential impact on individuals' rights and freedoms. However, the feared event 'exploitation of vulnerabilities' would be preliminary to the ones identified by CNIL (i.e., illegitimate access, unwanted change and disappearance of data), for it operates at a different level, i.e., at system level.

Moreover, following an all-encompassing interpretation of the CIA triad (see Chapter 2), the three security risks contemplated by the CNIL methodology would also take into account the security principles of authenticity, accountability, non-repudiation and reliability, therefore not limiting their scope to confidentiality, integrity and availability. An unwanted change of data is a breach of integrity, guarding against improper data modification and would therefore ensure *non-repudiation* and *authenticity*. On the other hand, the disappearance of data is a breach of availability, which aims to ensure *reliable* access to and use of data[1248].

All in all, the analysis of Art. 51 CSA showed that the CNIL methodology is flexible enough to cover the security objectives laid out in the Cybersecurity Act, thanks to both the various cybersecurity technical controls and a broader understanding of traditional information security risks.

5.2.2.3 The IoT generalisation test

Finally, the last issue under consideration is to what extent the CNIL methodology can be successfully transposed to and adopted by all IoT scenarios. When mapping the data flow in the first phase of the DPIA, the CNIL 'only' considers a simplified IoT interaction-model wherein machine-to-machine (M2M) communication is neglected.

Instead, in the fictional IoT device, the CNIL appears to be more preoccupied with human-to-machine communication (e.g., the child interacting with the connected toy, the parents monitoring the related data, etc.) and machine-to-manufacturer communication (e.g., data, recorded via sensors on the IoT device, are transferred to the mobile app, directly via the device or through the cloud servers, data analysis algorithms in the cloud generate the response data on the basis of previous dialogues and the

[1248] NIST, 'NISTIR 8074 - Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity' (n 154) 42–43.

interests detected and produce statistics on use and advertising targeting)[1249].

The lack of reference to the machine-to-machine (M2M) communication is a weakness of the methodology, for it is a core feature of IoT systems bearing on security and privacy.

On the one hand, it is a legitimate choice to conceive a fictional toy without the possibility of interaction with any other connected devices whatsoever; on the other hand, a DPIA methodology for IoT devices should also take this concern into consideration.

5.2.3 A rights-based data protection impact assessment methodology for IoT devices

The last section of the Chapter builds on previous ones with a view to drafting a DPIA methodology that could successfully integrate an assessment of the individuals' rights and freedoms impacted by personal data processing within a generalised IoT device. The resulting methodology is based on the guidance of Article 29 WP, ENISA and, particularly, the CNIL's specific IoT DPIA, bearing in mind the lessons learned in the previous section. For the sake of ensuring consistency with the CNIL methodology, on which in fact the model presented below builds on, the examples made to contextualise this methodology refer to a connected toy.

As seen in the above sections, the fair balance effort performed by supervisory authorities, EU agencies and private parties provides for a remarkable knowledge base which could easily be integrated into the CNIL methodology to better assess the risk to rights in such complex scenarios. Provided that the CNIL methodology satisfactorily operationalises the first two criteria of the WP29 guidelines on DPIAs, the model presented here can be almost completely superposed on Phases 1, 2 and 4 of the CNIL methodology. 'Almost', because the first step of the DPIA model would require some room for M2M communication in the functional description of the processing operation and main functionalities of the device under scrutiny.

A particular emphasis will be placed on the third criterion of the WP29 guidelines, which corresponds to phase 3 of the CNIL methodology – that has largely been dealt with in section 5.2.2.1, as it has not satisfactorily been addressed by the CNIL. The model presented in this section particularises CNIL's method for evaluating the impact on the identified risks by taking into account the methodology proposed by Mantelero, in particular, with regard to the assessment of the two risk components, i.e., severity and likelihood. Mantelero breaks down the two variables into their components to more meaningfully quantify their overall level.

Accordingly, the severity of the envisaged impacts is the combination of the gravity of the prejudice

[1249] CNIL, 'Privacy Impact Assessment (PIA) Methodology' (n 1199) 4–5.

in the exercising of the rights and freedoms, and the effort to overcome said consequences. On the other hand, the likelihood is estimated by considering the probability of a risk occurring and exposure, that is, the potential number of people at risk. The two couples of variables are then combined using a 4-step cardinal scale to estimate the overall likelihood and severity[1250].

In line with the outcomes of section 5.2.2.1, the assessment will go beyond the risks to privacy as addressed by the CNIL model, to explore the wider range of consequences on different rights and freedoms triggered by the IoT (a connected toy, in our – and CNIL's example) personal data processing, therefore ensuring full compliance to the requirement enshrined in Art. 35(7)(c) GDPR. In particular, a DPIA for a connected toy should also take into account an assessment of the risks to the right of parents to ensure the education and teaching of their children in conformity with their religious, philosophical and pedagogical convictions (Art. 14 CFR) and to the right to the integrity of the person (Art. 3 CFR), as previously discussed in section 5.2.2.1.

5.2.3.1 Step 1. Setting the context

General information

1.1 Product description:

The IoT device shall be broken down into all its components relevant to data processing as addressed in Chapter 1: from the device layer, including sensors and actuators (e.g., microphones, cameras, buttons, etc.), to the network and application layers (e.g., Wi-Fi connectivity, mobile app or online service, etc.).

1.2 Processing purposes:

The purposes of the processing must be detailed: e.g., interacting with the child, enabling the child to browse the internet and communicate with other users, etc.

1.3 Data controller(s) and data processor(s):

Data controllers and processors must be determined. For example, the manufacturer of the IoT device will be a data controller; data processors may be firms hosting and providing various services (e.g., device interactivity, data analysis, advertising, etc.).

Focus on personal data processing

1.4 Personal data processing:

[1250] Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (n 1190) 54–57.

The type (e.g., information about users, data entered in third-party app, data collected by the device, data provided by the device as a result of the interaction with the user based on life habits, advertising, etc.) and categories (e.g., common data, data relating to a minor, sensitive data according to Art. 9 GDPR, etc.) included in personal data processed; the recipients (e.g., controllers and processors); and the persons authorised to process said data.

1.5 Data supporting assets:

List of the hardware and software components on which data rely.

1.6 Lifecycle of data and processes:

For the sake of clarity, it is preferable to present the processes carried out *via* a diagram of data flows. This shall be complemented by a detailed description of the processing activities performed and how the product generally works, i.e., whether only human-to-machine interaction is foreseen or also machine-to-machine interaction, whether the data stay in the device for computation, or whether they are sent to cloud servers *via* a mobile app, whether a degree of AI is embedded in the system, etc.

5.2.3.2 Step 2. Assessment of the necessity and proportionality of the processing

Assessment of the necessity and proportionality of the processing

2.1 Purposes:

The purposes of each data processing operation must be explained and justified (e.g., third-party sharing, profiling, provision of primary service, etc.), according to Art. 5(1)(b) GDPR.

2.2 Legal basis:

A suitable legal basis (Art. 6, 9 GDPR) shall be chosen for each processing operation. As noticed by the CNIL model, "there can be several types of bases for a processing operation: for example, a contract associated with the purchase of a product for using it for its primary purpose and consent for its secondary purposes (improving the service, marketing, etc.) which will be obtained when the product is activated"[1251].

2.3 Data minimisation:

Firstly, the amount of personal data that will be processed shall be limited to what is strictly necessary for the purposes of the processing (Art. 5(1)(c) GDPR). Secondly, technical and organisational measures can be adopted to further minimise the sensitivity of the processing (e.g., pseudonymisation, randomisation, etc.).

[1251] CNIL, 'PIA: Application to IoT Devices' (n 1198) 9.

2.4 Data quality:

Data must be accurate and kept up to date (Art. 5(1)(d) GDPR).

2.5 Storage limitation:

For each type of data, a storage limitation period, and also an erasure mechanism must be set (Art. 5(1)(e) GDPR).

Assessment of the measures guaranteeing data subjects' rights

2.6 Information for the data subjects:

Measures to provide information to users (or their parents, if applicable), as provided for in Articles 12, 13 and 14 GDPR. These measures include the presentation, at the moment of activation and thereafter, of legible and easy-to-understand terms and conditions; a detailed and easy-to-understand description of the processing purposes and data flows; a detailed presentation of the data collected, inferred, processed and transmitted (e.g., to third parties), etc. In this regard, see in particular section 4.1.2.

2.7 Measures on consent:

If the processing is based on consent, measures to ensure compliance with consent requirements must be in place (Articles 7 and 8 GDPR). These may include: granular and specific consent *per* data category or processing type; presentation in an intelligible and easy-to-understand language adapted to the target user (particularly for children); parents' consent for minors under the age of 13 years, consent can be withdrawn easily and at any time. Against the background of technical solutions to facilitate consent in IoT systems, see section 4.1.1.

2.8 Rights of access and to data portability:

Measures to implement the rights of access (Art. 15 GDPR) and to data portability (Art. 20 GDPR) on the device. These may include the possibility of accessing (and downloading) all the users' personal data and retrieving, in an easily reusable format, personal data provided by the user.

2.9 Right to rectification and to erasure:

Measures to implement the rights to rectification (Art. 16 GDPR) and erasure (Art. 17 GDPR) on the device. These may include easily understandable information about how to erase data, also remotely in the event that the device is lost.

2.10 Right to object and to restriction of processing:

Measures to implement the rights to object (Art. 18 GDPR) and to restriction of processing (Art. 21 GDPR) on the device. These may include a notification to change the default privacy settings when activating the device; a parental control system for children; the possibility of deactivating some of the device's features; compliance with legal requirements and DPA guidelines related to tracking technologies, such as cookies.

2.11 Geo-localisation of the processing:

Several legal arrangements must be implemented, depending on the country where the personal data are stored i.e., whether outside the EU or not.

5.2.3.3 Step 3. Assessment of the risks to rights and freedoms of data subjects

Risk Assessment

3.1 Risk to the right to privacy and protection of personal data (Articles 7 and 8 CFR; Art. 8 ECHR):

- determine the risk sources: e.g., rogue neighbour; hackers; negligent or rogue user/family member/friend; AI-processed/predetermined sentences at the base of the interaction between the toy and the user.

- determine the main threats: e.g., illegitimate access to personal data; unwanted change of personal data; disappearance of personal data; intrusion of the toy into the user's private sphere.

- determine the potential impacts: e.g., profiling; targeted advertising; identity theft; loss of history and personal service settings; provision of unexpected content – including sensitive personal data – by the user when interacting with the toy.

- determine the severity: taking into account the above, estimate the gravity of the prejudice to the right assessed and the effort to overcome it on a scale of 1 to 4, where 1 corresponds to low; 2 to medium; 3 to high; 4 to very high. Then, combine the two variables to obtain the overall level of the severity (1-2: low; 3-6: medium; 8-9: high; 12-16: very high).

- determine the likelihood: taking into account the above, estimate the probability of the risk occurring and the exposure on a scale of 1 to 4, where 1 corresponds to low; 2 to medium; 3 to high; 4 to very high. Then, combine the two variables to obtain the overall level of the likelihood (1-2: low; 3-6: medium; 8-9: high; 12-16: very high).

- overall risk level of the initial assessment: taking into account the severity and the likelihood, the overall impact for each risk is determined by rounding up: low-low= low; low-medium= medium; low-high=medium; low-very high=medium; medium-high= high; medium-very high= high; high-very high= very high; very high-very high= very high.

3.2 Risk to the right to the integrity of the person (Art. 3 CFR):

- determine the risk sources: e.g., hackers; rogue neighbours; malfunctions.

- determine the main threats: e.g., malicious attacks on the connected product.

- determine the potential impacts: e.g., physical harm (depending on the actual size and characteristics of the toy); physiological harm.

- determine the severity: taking into account the above, estimate the gravity of the prejudice to the right assessed and the effort to overcome it on a scale of 1 to 4, where 1 corresponds to low; 2 to medium; 3 to high; 4 to very high. Then, combine the two variables to obtain the overall level of the severity (1-2: low; 3-6: medium; 8-9: high; 12-16: very high).

- determine the likelihood: taking into account the above, estimate the probability of the risk occurring and the exposure on a scale of 1 to 4, where 1 corresponds to low; 2 to medium; 3 to high; 4 to very high. Then, combine the two variables to obtain the overall level of the likelihood (1-2: low; 3-6: medium; 8-9: high; 12-16: very high).

- overall risk level of the initial assessment: taking into account the severity and the likelihood, the overall impact for each risk is determined by rounding up: low-low= low; low-medium= medium; low-high=medium; low-very high=medium; medium-high= high; medium-very high= high; high-very high= very high; very high-very high= very high.

3.3 Risk to the right to education (Art. 14 CFR):

- determine the risk sources: e.g., manufacturer's choices; AI embedded in the IoT product (if any).

- determine the main threats: e.g., transmission of value-oriented content to the user interacting with the connected toy.

- determine the potential impacts: e.g., limitation to parents' right to ensure moral and religious education of their children in accordance with their religious, philosophical and pedagogical convictions.

- determine the severity: taking into account the above, estimate the gravity of the prejudice to the right assessed and the effort to overcome it on a scale of 1 to 4, where 1 corresponds to low; 2 to medium; 3 to high; 4 to very high. Then, combine the two variables to obtain the overall level of the severity (1-2: low; 3-6: medium; 8-9: high; 12-16: very high).

- determine the likelihood: taking into account the above, estimate the probability of the risk occurring and the exposure on a scale of 1 to 4, where 1 corresponds to low; 2 to medium; 3 to high; 4 to very high. Then, combine the two variables to obtain the overall level of the likelihood (1-2: low; 3-6: medium; 8-9: high; 12-16: very high).

- overall risk level of the initial assessment: taking into account the severity and the likelihood, the overall impact for each risk is determined by rounding up: low-low= low; low-medium= medium; low-high=medium; low-very high=medium; medium-high= high; medium-very high= high; high-very high= very high; very high-very high= very high.

Assessment of technical and organisational mitigation measures and re-assessment for each identified risk

3.x Technical measures regarding the personal data being processed:

To mitigate the risks found, detail here the technical security measures implemented in the processing of personal data adopted: e.g., end-to-end encryption; pseudonymisation; anonymisation; access control; two-factors authentication; etc[1252].

3.x Technical measures regarding the system where the processing is carried out:

To mitigate the risks found, detail here the technical security measures implemented in the system adopted: e.g., hardware authentication; access logging; storage duration; backups; operating security; etc[1253].

3.x Organisational measures:

Detail here the organisational mitigation measures adopted: e.g., closed set of communication input for the connected product; possibility to access, verify and modify the pre-installed phrases at the basis of the communication between the connected toy and the user (the child); possibility to deactivate sensing/monitoring features of the device; excluding interaction with other IoT devices; etc.

3.x Re-assessment

In light of the mitigation measures adopted, the risk assessment shall be performed again to determine the final impact on the rights and freedoms of natural persons brought about by the personal data processing performed by the connected product scrutinised.

5.2.3.4 Step 4. Involvement of stakeholders

Preparation of the documentation for validation

4.1 Consolidate the DPIA's findings through a visual presentation of each step.

[1252] ENISA (n 92): see Annex A.

[1253] ibid.

4.2 Document the consideration of stakeholders: the advice of the person in charge of ‘data protection’ aspects (Art. 35(2) GDPR) and the view of data subjects or their representatives (Art. 35(9) GDPR).

Formal validation

4.3 Taking into account the selected measures, the residual risks and the considerations of stakeholders, the DPIA may be validated; conditional on improvement; refused, alongside the underlying processing.

5.3 Conclusion

This Chapter dwelt on the GDPR’s requirement to carry out a data protection impact assessment (DPIA). In particular, it broke down Art. 35 GDPR into all its components, stressing the centrality of the requirement to manage ‘the risks to the rights and freedoms of data subjects’ (Art. 35(7)(c) GDPR).

Existing DPIA models, even those provided by data protection authorities, tend to limit the scope of this obligation to an assessment of the impact on the sole right to privacy, without departing from the ‘pre-GDPR approach’ of privacy impact assessments (PIAs) that used to focus on aspects such as data quality and security. This approach is arguably more aligned with traditional information security risk assessments, such as the ISO group of privacy standards, which nonetheless differ in scope and rationale from the standard set by EU data protection law i.e., the GDPR.

Hence, the analysis demonstrated that a more meaningful interpretation of the Regulation should go beyond only upholding the right to privacy and the protection of personal data, to encompass, in line with Art. 1(2) GDPR, the full catalogue of the EU fundamental rights framework.

Against this backdrop, this chapter presented an original DPIA methodology for connected devices (IoT). It builds on the CNIL model which fell short of implementing the requirement of assessing the impact of risks to ‘the rights and freedoms of data subjects’. The last section of this Chapter presents a holistic ‘rights-based’ DPIA methodology for an IoT device, with the underlying hope of providing useful guidelines for technology development and improved compliance with GDPR requirements, too often interpreted as a ‘ticking-the-box’ exercise, in line with a more consolidated information security tradition.

The main contribution of this chapter is indeed represented by a DPIA methodology including the assessment of the impact on different rights and freedoms that have been deemed to be relevant to

the specific nature of the given application i.e., a connected toy – to ensure continuity with the CNIL model.

Some might argue that this methodology would represent an additional burden for economic operators involved in the IoT and AI industry. Considering the full catalogue of fundamental rights and freedoms enshrined in EU primary law would, in fact, set the threshold too high. Moreover, the line of reasoning behind a broad interpretation of Art. 35(7)(c) GDPR can to some extent contribute to 'distort' the rationale of data protection law, which inevitably becomes '*the law of everything*': "complying with and enforcing such a law in a meaningful way is impossible, and something – enforcement or compliance – will have to give"[1254].

However, it can be argued that applying the requirement of Art. 35 GDPR to the letter would not be disproportionate for manufacturers-as-data controllers vis-à-vis the risks they bring to society and the profits they make out of it, building on the long-standing tradition of law and economics theories[1255]. Furthermore, the adoption of these types of holistic methodologies presents data controllers with an opportunity in the form of competitive advantage compared to competitors that do not operationalise and specify vague GDPR requirements, such as Art. 35(7)(c)[1256].

[1254] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 1003) 77.

[1255] Robert D Cooter, 'Economic Theories of Legal Liability' (1991) 5 Journal of Economic Perspectives 11, 11.

[1256] Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (n 1190) 32; Gloria González Fuster, Rosamunde Van Brakel and Paul De Hert, 'Co-Regulation and Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and Data Protection-by-Design' in Gloria González Fuster, Rosamunde van Brakel and Paul De Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar Publishing 2022).

Conclusion and Future Paths

This work started with several open questions. To begin with, efforts towards a common definition of 'Internet of Things', and resource-constrained devices more specifically, are still on-going. Also, from a theoretical and definitional standpoint, further reflections are still needed to map out the exact boundaries of the concepts of security, cybersecurity, safety and privacy – and the underlying relationships between them – in light of the ubiquitous IoT. Having regard to cybersecurity and safety in particular, given that EU cybersecurity law is still in its infancy, enforceable cybersecurity rules need to be strengthened. Against the background of the fast-evolving European cybersecurity regulatory framework – including the revision of the NIS Directive and several pieces of product safety legislation and the proposal for a Cyber Resilience Act (CRA), coherence within the EU cybersecurity *acquis* shall be ensured, especially in view of isolated moves forwarded by Member States to respond to the fast-paced digital threat landscape[1257]. On the other hand, EU privacy and data protection laws should also be (re-)assessed to investigate whether they are up to the challenges brought about by the structural data and metadata processing of IoT systems. Lastly, if, while awaiting the adoption of the CRA, a common EU-wide approach to address the cybersecurity risk in IoT is still missing, existing data protection risk assessment models do not encompass the full breadth and depth of the standard set by the GDPR, in particular, taking into account the requirement to assess the risks to the rights and freedoms of data subjects enshrined in Art. 35(7)(c) GDPR.

The added value of this research lies in the critical analysis of the values underpinning the EU legal frameworks on *security and privacy*, against the backdrop of the IoT paradigm shift blurring the boundaries between the digital and the physical dimensions. By introducing the current technical landscape (Chapter 1) and exploring the interwoven dimension of cybersecurity and privacy (Chapter 2), the thesis aimed to (i) bridge the communication gap between technical and legal communities; (ii) address the relevant regulatory gaps in EU 'security and privacy' legal frameworks vis-à-vis the challenges brought about by the IoT; (iii) design a holistic risk assessment methodology that brings together traditional information security frameworks and the GDPR rights-based approach.

With this in mind, Chapter 1 provided a working definition and architecture taxonomy of the 'Internet of Things' and 'resource-constrained devices', coupled with a threat landscape where each specific attack is linked to a layer of the taxonomy. Chapter 2 laid down the theoretical foundations for an interdisciplinary approach and a unified, holistic vision of cybersecurity, safety and privacy justified by the 'IoT revolution' through the so-called *infraethical* perspective. Cybersecurity, conceived as an

[1257] Schmitz-berndt and Chiara (n 829).

instrumental value, can *facilitate* or *hinder* the enjoyment of fundamental values, such as fundamental rights and personal safety, depending on how different types of cybersecurity policies and technical controls have been designed and set up.

Chapter 3 investigated whether and to what extent the fast-evolving European cybersecurity regulatory framework addresses the security challenges brought about by the IoT by allocating legal responsibilities to the right parties. The critical analysis of the EU cybersecurity *acquis,* which does not target IoT products specifically and comprehensively, culminated with an overview of the CRA proposal. This horizontal legislation on cybersecurity for products with digital elements, building on the principles and structures of the NLF, is the last piece of the jigsaw, ensuring coherence in the EU legal frameworks regulating (connected) products cybersecurity.

Chapters 4 and 5, on the other hand, focused on 'privacy' understood by proxy to include EU data protection. In particular, Chapter 4 addressed three legal challenges brought about by the ubiquitous IoT data and metadata processing to EU privacy and data protection legal frameworks i.e., the ePrivacy Directive and the GDPR. In the same vein as Chapter 3, the critical analysis came to the conclusion that European privacy law is incomplete without a reform of the ePrivacy Directive. Chapter 5 cast light on the risk management tool enshrined in EU data protection law, or rather, the Data Protection Impact Assessment (DPIA). After concluding that existing DPIA models (even those designed specifically for IoT devices) are too narrowly focused on assessing only risks to the right to privacy – without fulfilling the requirement to manage 'the risks to the rights and freedoms', an original DPIA methodology for connected devices was proposed, building on the CNIL model.

Whereas legal research at the intersection of the IoT and data protection has been flourishing in the recent years[1258], future research in EU cybersecurity law should explore and strengthen the theoretical foundations underlying the discussion towards a new fundamental right to cybersecurity. Cybersecurity does not figure as a policy field in the EU Treaties, nor there is an explicit legal basis for EU policy in this regulatory area. Henceforth, the legal basis for EU policy in this area has been predominantly the functioning of the internal market in accordance with Art. 114 TFUE (as seen in

[1258] Noto La Diega (n 904) 274. See also Irene Ioannidou and Nicolas Sklavos, 'On General Data Protection Regulation Vulnerabilities and Privacy Issues , for Wearable Devices and Fitness Tracking Applications' (2021) 5 Cryptography; Lachlan Urquhart, Tom Lodge and Andy Crabtree, 'Demonstrably Doing Accountability in the Internet of Things' (2019) 27 International Journal of Law and Information Technology 1; Leonie Tanczer and others, 'IoT and Its Implications for Informed Consent - PETRAS IoT Hub, STEaPP' (2017) <https://discovery.ucl.ac.uk/id/eprint/10050101/1/IoTandConsent_PM_Workshop_Report - 11Comp.pdf> accessed 21 October 2022; Jeremy Siegel, 'When the Internet of Things Flounders: Looking into GDPR-Esque Security Standards for IoT Devices in the United States from the Consumers' Perspective' (2020) 20 Journal of High Technology Law 189; Sandra Wachter, 'The GDPR and the Internet of Things: A Three-Step Transparency Model' (2018) 10 Law, Innovation and Technology 266.

Chapter 3)[1259]. Taking into account the seminal article by Vagelis Papakonstantinou – who first attempted to lay down the groundwork with a view to formally acknowledging this new right in EU law in 2022 [1260], this thesis contributed to the debate from a twofold perspective.

Without dwelling on the distinction between *cybersecurity-as-praxis* and *cybersecurity-as-a-state*, used by Papakonstantinou as a proxy for developing a doctrine underpinning the establishment of this new fundamental right, here it is enough to map out relevant takeaways from this thesis to some corollaries of the legal challenges raised by the theory for a right to cybersecurity. In particular, the first challenge hinges on the relationship between *cybersecurity* and *security*, and, whether the former could be subsumed under the latter. The second one entails the actual legal remedies that EU cybersecurity law place at the disposal of individuals if cybersecurity threats actually occur.

Papakonstantinou concludes that the concept of cybersecurity and security differ, "because security includes real-world circumstances, protecting against real-world threats, while cybersecurity refers to the digital realm, protecting from cyber threats"[1261]. More interesting is what follows. "The two set of threats do not necessarily coincide. While a time may well be imagined that the real and the digital converge, until such time cybersecurity and security, although sharing the same linguistic root and interpretational difficulties, should be treated as two different concepts and rights, each to be assessed by its own merit"[1262].

In this regard, Chapter 2 attempted to cast some light on this entanglement. IoT hyper-interconnectedness has been conceived throughout this thesis as a game-changer, for it intertwines cybersecurity and security more than ever before. Indeed, the IoT ultimately blurs the boundaries between the *digital* and the *physical.* The assets traditionally protected by cybersecurity and security increasingly overlap. Risk factors and threats in today's hyper-connected digital environment go beyond the technological infrastructure of information systems, networks and the underlying information. Cyberattacks could also infringe individuals' fundamental rights, impair physical safety and have critical consequences for services, institutions and communities. On the one hand, some could easily conclude that "there would be no need for a new right to cybersecurity because the general right to security is enough"[1263]. I argue on the other hand that the paradigm shift outlined in

---

[1259] Jed Odermatt, 'The European Union as a Cybersecurity Actor' in Steven Blockmans and Panos Koutrakos (eds), *Research Handbook on EU Common Foreign and Security Policy* (Edward Elgar Publishing 2018) 359.

[1260] Papakonstantinou (n 1163). On a comparative note see: Scott J Shackelford, 'Should Cybersecurity Be a Human Right? Exploring the "Shared Responsibility" of Cyber Peace' (2019) 55 Stanford Journal of International Law 158; Ido Kilovaty, 'An Extraterritorial Human Right to Cybersecurity' (2020) 10 Notre Dame Journal of International & Comparative Law 35.

[1261] Papakonstantinou (n 1163) 7.

[1262] ibid 7–8.

[1263] ibid 7.

Chapter 2 would rather call for reinforcement of the general EU fundamental right to security, either by introducing a right to cybersecurity in new EU law or amending Art. 6 of the EU Charter of Fundamental Rights, as suggested by Papakonstantinou.

But, why introducing this new right? In this respect, the second legal challenge hinges on examining whether the existing (and proposed) legislative instruments justify this doctrine, in particular, taking into account the remedies granted to individuals if the addressees of EU cybersecurity legislation infringe the legal duties they shall comply with. Papakonstantinou looked deeper into the NISD and the EU Cybersecurity Act, the only EU horizontal legal acts in the cybersecurity area as the Cyber Resilience Act proposal had not yet been published. The analysis provided by Chapter 3 clearly shows that both the NIS Directive (and the NIS2) and the Cybersecurity Act do not afford any rights nor other means of protection to individuals. These legal acts have thus their primary objectives in the 'functioning of the internal market', that is, not the protection of natural and legal persons per se. As already stated, the CRA also finds its legal basis in Art. 114 TFEU. Like the NIS Directive(s) and the Cybersecurity Act, the CRA proposal does not provide any remedies for individuals, contrary to the expectations of the EU consumer association BEUC[1264]. Without this, consumers that have suffered damage caused by the infringements of relevant CRA cybersecurity obligations by economic operators would have to resort to national product liability legal frameworks (e.g., the Italian consumer code[1265]).

From a law-making perspective, the right to cybersecurity – the basic components of which shall find their grounds in the rights-based approach to cybersecurity enshrined in the broad definition provided by Art. 2(1) Cybersecurity Act (see Chapter 2) – may be introduced in the Cyber Resilience Act, rather than in the Cybersecurity Act or the NIS2[1266], given its current legal status i.e., a legislative proposal. This, in turn, would facilitate the affordance of legal remedies and means of redress for consumers if a cybersecurity threat is realised and, consequently, damages occur. By using EU personal data protection law as a point of reference, and, in particular, 1995 EU Data Protection Directive – which was based on the predecessor of Art. 114 TFEU, Papakonstantinou remarks that "it is not necessary first for a new right to be spelled out in the Treaties, in order for secondary legislation to further detail its particulars. As personal data protection has demonstrated, a Directive (or, a Regulation, for example the EU Cybersecurity Act) could well grant to Europeans rights and obligations akin to a right, before a right per se finds its way into the Treaties"[1267].

[1264] BEUC (n 815) 12.

[1265] Daniele Vecchi and Michela Turra, 'Italy' in Clinton Davis Varner and Madison Kitchens (eds), *The Product Regulation and Liability Review* (7th edn, Law Business Research Ltd 2020).

[1266] Papakonstantinou (n 1163) 13.

[1267] ibid.

A right to cybersecurity in EU law would best guide the fast-growing regulatory landscape (addressed in Chapter 3) and support the emergence of the new policy field of EU cybersecurity law[1268]. EU cybersecurity law has shifted relatively recently, that is from the adoption of the Cybersecurity Act in 2019, from organisational and technical legislation to comprehensive multi-level and multi-stakeholder regulatory approach. The EU Commission Cybersecurity Strategy for a Digital Decade from 2020 advocates for and promotes structured exchanges and cooperation between stakeholders, including the private sector, academia and civil society[1269].

Within the scope of cybersecurity as a shared responsibility (see Chapter 2), the public sector enacted, on the one hand, legal frameworks to facilitate the development of standards and certification (Cybersecurity Act) and, on the other hand, legislation to enhance the level of security vis-à-vis entities that are essential to the functioning of our societies (NIS2 Directive) and economic operators involved in the manufacturing of products (Cyber Resilience Act). At the same time, "the private sector bears the responsibility of designing robust systems, developing and improving methods to foster robustness of the services and products that they offer, and collaborating with the public sector for the controlling and testing mechanisms"[1270].

In this respect, on 17 October 2022, Member States approved Council conclusions with a view to strengthening the security of ICT supply chains[1271]. Against the background of future highly likely supply chain cyberattacks (see Chapter 1), the Council acknowledges the need to maximise and streamline the use of existing EU instruments and approaches to achieve these objectives as well as the need to continually adapt to the changing cyber threat landscape by introducing additional suitable measures and mechanisms[1272].

Beside the need to align existing and forthcoming supply chain cybersecurity requirements under different legislative instruments (i.e., Cybersecurity Act, NIS2 and Cyber Resilience Act), as addressed in Chapter 3, particular emphasis is placed on public procurement: the Commission is invited by the Council to develop methodological guidelines in order to encourage the contracting authorities to place appropriate focus on the cybersecurity practices of tenderers and their subcontractors, and assess or revise – if needed – relevant public procurement legislation[1273].

[1268] Ramses A Wessel, 'Towards EU Cybersecurity Law: Regulating a New Policy Field' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing Ltd 2015).

[1269] European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy (n 619) 23.

[1270] Taddeo (n 225) 351.

[1271] Council of the European Union, 'Council Conclusions on ICT Supply Chain Security', vol 13664/22 (2022) <https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf>.

[1272] ibid 6.

[1273] ibid 7.

Drawing on the lessons from the consequences of strategic dependencies of the EU single market on foreign-country resources, from fossil fuels to rare earths (the latter in particular urged EU action in the form of a European Chips Act[1274] and European Critical Raw Materials Act[1275], announced in the 2022 EU State of the Union Address by President Von der Leyen), as well as from the impacts of the disruptions in supply chains during the COVID-19 pandemic, efforts shall be made to avoid unwanted strategic external dependencies in relation to ICT products and services which, eventually, form part of the IoT.

[1274] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act) COM/2022/46 final.

[1275] European Commission, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_5523.

Bibliography

Abbate J, *Inventing the Internet* (MIT Press 1999)

Acar A and others, 'Peek-a-Boo: I See Your Smart Home Activities, Even Encrypted!' [2020] WiSec 2020 - Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks 207

AEPD, 'Data Protection and Security' (*Prensa y comunicación*, 2020) <https://www.aepd.es/en/prensa-y-comunicacion/blog/data-protection-and-security>

——, 'IoT (I): What Is IoT and Which Risks Does It Entail' (2020) <https://www.aepd.es/en/prensa-y-comunicacion/blog/iot- and-which-risks-does-it-entail>

AIOTI, 'AIOTI Position on the EU Cybersecurity Act Proposal' (2018) <https://euagenda.eu/publications/aioti-position-on-the-eu-cybersecurity-act-proposal> accessed 8 December 2021

——, 'High Level Architecture (HLA) AIOTI WG03-LoT Standardisation' (2018)

——, 'AIOTI Feedback to the Public Consultation on the Revised Draft NIS Directive (NIS2)' (2021) <https://ec.europa.eu/digital-single-market/en/news/aioti-> accessed 8 December 2021

Alani MM, *Guide to OSI and TCP/IP Models* (Springer International Publishing 2014) <http://link.springer.com/10.1007/978-3-319-05152-9> accessed 20 September 2021

Albrecht JP, 'How the GDPR Will Change the World' (2016) 2 European Data Protection Law Review 287

ANASTACIA Project, 'Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures ' (*2019*) <https://cordis.europa.eu/project/id/731558> accessed 29 August 2022

Anderson S and Williams T, 'Cybersecurity and Medical Devices: Are the ISO/IEC 80001-2-2 Technical Controls up to the Challenge?' (2018) 56 Computer Standards & Interfaces 134

ANEC, 'ANEC Response to EC Call for Evidence for an Impact Assessment on the Cyber Resilience Act (CRA) Initiative' (2022) <https://www.anec.eu/images/Publications/position-papers/Digital/ANEC-2022-DIGITAL-CYBER-006.pdf>

ANEC and BEUC, 'Keeping Consumers Safe from Dangerous Products: How to Make the General Product Safety Regulation a Useful Tool to Ensure Product Safety' (2021) <https://www.beuc.eu/publications/beuc-x-2021-107_general_product_safety_regulation_a_useful_tool_to_ensure_product_safety.pdf>

Anglmayer I, ‘Briefing Implementation Appraisal EPRS, Machinery Directive: Revision of Directive 2006/42/EC’ (2021) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2021)694206 > accessed 18 October 2021

Antonakakis M and others, ‘Understanding the Mirai Botnet’, *26th USENIX Security Symposium* (2017) <http://ipads.se.sjtu.edu.cn/lib/exe/fetch.php?media=publications:vtz.pdf%0Ahttps://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/hua> accessed 20 September 2021

Apthorpe N and others, ‘Keeping the Smart Home Private with Smart(Er) IoT Traffic Shaping’ (2019) 3 Proceedings on Privacy Enhancing Technologies 128

Apthorpe N, Reisman D and Feamster N, ‘A Smart Home Is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic’ [2017] arXiv <https://arxiv.org/pdf/1705.06805.pdf> accessed 3 June 2022

Apthorpe NJ, ‘Network Privacy and User Protection in the Internet of Things’ (Princeton University 2020) <https://search.proquest.com/dissertations-theses/network-privacy-user-protection-internet-things/docview/2427502325/se-2?accountid=13042%0Ahttp://oxfordsfx.hosted.exlibrisgroup.com/oxford?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&g>

Article 29 Data Protection Working Party, ‘Opinion 04/2007 on the Concept of Personal Data’ (2007)

——, ‘Opinion 03/2013 on Purpose Limitation’ (2013) <http://ec.europa.eu/justice/data-protection/index_en.htm> accessed 6 May 2022

——, ‘Opinion 05/2014 on Anonymisation Techniques’ (2014) <http://ec.europa.eu/justice/data-protection/index_en.htm%0Ahttp://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 17 February 2020

——, ‘Opinion 8/2014 on the Recent Developments on the Internet of Things’ (2014) <http://ec.europa.eu/justice/data-protection/index_en.htm> accessed 31 January 2020

——, ‘Opinion 9/2014 on the Application of Directive 2002/58/EC to Device Fingerprinting’ (2014)

——, ‘Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks’ (2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>

——, ‘Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679’, vol WP

248 rev (2017) <https://ec.europa.eu/newsroom/article29/items/611236/en>

——, ‘Opinion 01/2017 on the Proposed Regulation for the EPrivacy Regulation (2002/58/EC)’ (2017)

——, ‘Guidelines on Consent under Regulation 2016/679’ (2018)

Banasinski C and Rojszczak M, ‘Cybersecurity of Consumer Products against the Background of the EU Model of Cyberspace Protection’ (2021) 00 Journal of Cybersecurity 1 <https://academic.oup.com/cybersecurity/article/7/1/tyab011/6262024> accessed 28 December 2021

Banca d’Italia G di coordinamento sulla sicurezza cibernetica (GCSC), ‘Sicurezza Cibernetica: Il Contributo Della Banca d’Italia e Dell’Ivass ’ (2018) <https://www.bancaditalia.it/pubblicazioni/tematiche-istituzionali/2018-sicurezza-cibernetica/Tem_Istituzionali_sicurezza_cibernetica_agosto_2018.pdf> accessed 5 October 2021

Barak B and Brakerski Z, ‘The Swiss Army Knife of Cryptography ’ (*Windows on Theory - A Research Blog*, 2012) <https://windowsontheory.org/2012/05/01/the-swiss-army-knife-of-cryptography/> accessed 7 April 2022

BDI, ‘EU-Wide Cybersecurity Requirements: Introduction of Horizontal Cybersecurity Requirements Based on the New Legislative Framework and Bridge to the EU Cybersecurity Act’ (2021) <https://www.din.de/resource/blob/788018/f9708b36c89b2e527bcb1a66f523827a/2021-bdi-din-dke-position-cybersicherheit-europa-en-final-data.pdf> accessed 6 June 2022

——, ‘Position Paper on NIS 2-Directive’ (2021)

Ben Dhia S, Ramdani M and Sicard E, *Electromagnetic Compatibility of Integrated Circuits* (Sonia Ben Dhia, Mohamed Ramdani and Etienne Sicard eds, Springer US 2006)

Benjamin W, *Walter Benjamin: Selected Writings, 1: 1913-1926* (Marcus Paul Bullock and Michael William Jennings eds, Harvard University Press 2004) <http://www.riss.kr/link?id=M12705986> accessed 19 October 2021

Bernes A, ‘Enhancing Transparency of Data Processing and Data Subject’s Rights Through Technical Tools: The PIMS and PDS Solution’ in Roberto Senigaglia, Claudia Irti and Alessandro Bernes (eds), *Privacy and Data Protection in Software Services* (Springer Nature 2022)

Bertino E, ‘Security and Privacy in the IoT’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Springer Verlag 2018)

Bertoldi P and Serrenho T, ‘Smart Home and Appliances: State of the Art - Energy, Communications, Protocols, Standards’ (Publications Office of the European Union 2019)

BEUC, ‘Cyber Resilience Act: Cybersecurity of Digital Products and Ancillary Services - BEUC Response to Public Consultation’ (2022) <https://www.beuc.eu/publications/beuc-x-2022-051_cyber_resilience_act_public_consultation_beuc_position_paper.pdf>

Biasin E, ‘The NIS2 Proposal: Which Regulatory Challenges for Healthcare Cybersecurity?’ (*KU Leuven CiTiP blog*, 2021) <https://www.law.kuleuven.be/citip/blog/the-nis2-proposal-which-regulatory-challenges-for-healthcare-cybersecurity/>

Biasin E and Kamenjašević E, ‘Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals’ (2022) 3 International Cybersecurity Law Review 163

Biega AJ and Finck M, ‘Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems’ [2021] Technology and Regulation 44 <https://doi.org/10.26116/techreg.2021.004> accessed 3 May 2022

Bincoletto G, *Data Protection by Design in the E-Health Care Sector*, vol 22 (Luxembourg Legal St…, Nomos 2021)

Bishop M, ‘About Penetration Testing’ (2007) 5 IEEE Security and Privacy 84

Bitkom, ‘Cyber Resilience Act (CRA)’ (2022) <https://www.bitkom.org/EN/List-and-detailpages/Publications/Position-Paper-Cyber-Resilience-Act>

Blind K, ‘The Impact of Standardisation and Standards on Innovation’ in Jakob Edler and others (eds), *Handbook of Innovation Policy Impact* (Edward Elgar Publishing Ltd 2016)

Blythe JM, Johnson SD and Manning M, ‘What Is Security Worth to Consumers? Investigating Willingness to Pay for Secure Internet of Things Devices’ (2020) 9 Crime Science 1 <https://link.springer.com/articles/10.1186/s40163-019-0110-3> accessed 22 December 2021

Bobbio N, *Future of Democracy* (Richard Dellamy and Roger Griffin (translated by) eds, Wiley Polity 1987)

Body of European Regulators for Electronic Communication, ‘Report on OTT Services’ (2016) <https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5751-berec-report-on-ott-services_0.pdf>

Borghetti J-S, ‘How Can Artificial Intelligence Be Defective?’ in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things - Münster Colloquia on EU Law and the Digital Economy IV* (Bloomsbury Publishing 2019)

Borgogno O and Colangelo G, ‘SEPs Licensing Across the Supply Chain: An Antitrust Perspective’ [2021] SSRN Electronic Journal <https://papers.ssrn.com/abstract=3766118> accessed 29 November 2021

Bormann, C., Ersue, M., & Keranen A, 'RFC 7228: Terminology for Constrained-Node Networks', vol 39 (2014) <http://dx.doi.org/10.1016/j.biochi.2015.03.025%0Ahttp://dx.doi.org/10.1038/nature10402%0Ahttp://dx.doi.org/10.1038/nature21059%0Ahttp://journal.stainkudus.ac.id/index.php/equilibrium/article/view/1268/1127%0Ahttp://dx.doi.org/10.1038/nrmicro2577%0Ahttp://> accessed 31 January 2020

Bossong R and Wagner B, 'A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union' in Oldrich Bures and Helena Carrapico (eds), *Security Privatization: How Non-Security-Related Private Businesses Shape Security Governance* (Springer International Publishing 2018)

Böttinger K, Schuster D and Eckert C, 'Detecting Fingerprinted Data in TLS Traffic', *ASIACCS 2015 - Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (Association for Computing Machinery 2015)

Boyens J and others, 'Supply Chain Risk Management Practices for Federal Information Systems and Organizations' (2015) <http://dx.doi.org/10.6028/NIST.SP.800-161> accessed 20 September 2021

Brighi R, 'Cibercrimine e Anonimato in Rete. Riflessioni Su Sicurezza, Efficacia Investigativa e Tutela Delle Libertà Personali' [2017] Sicurezza e Scienze Sociali 29 <http://www.francoangeli.it/Riviste/SchedaRivista.aspx?IDarticolo=61321&lingua=IT> accessed 2 October 2021

——, 'Cybersecurity. Dimensione Pubblica e Privata Della Sicurezza Dei Dati' in Thomas Casadei and Stefano Pietropaoli (eds), *Diritto e Tecnologie Informatiche - Questioni di Informatica Giuridica, Prospettive Istituzionali e Sfide Sociali* (Cedam 2021)

Brighi R and Chiara PG, 'La Cybersecurity Come Bene Pubblico: Alcune Riflessioni Normative a Partire Dai Recenti Sviluppi Nel Diritto Dell'Unione Europea' (2021) 21 Federalismi.it 18

Brooks RR, *Introduction to Computer and Network Security: Navigating Shades of Gray* (1st Editio, Chapman and Hall/CRC Routledge 2014)

Bruno B, 'Cybersecurity Tra Legislazioni, Interessi Nazionali e Mercato' (2020) 14 Federalismi.it

BSA The Software Alliance, 'Comments on EU Commission's NIS Directive Review' (*2020*) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F543319_it> accessed 3 December 2021

Burton C, 'Article 32 Security of Processing' in Christopher; Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

——, ‘Article 33 Notification of a Personal Data Breach to the Supervisory Authority’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Bygrave LA, ‘Article 25 Data Protection by Design and by Default’ in Christopher; Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Bygrave LA and Schartum DW, ‘Consent, Proportionality and Collective Power’, *Reinventing Data Protection?* (Springer Netherlands 2009)

Bygrave LA and Tosoni L, ‘Article 4(11). Consent’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press 2020)

C.A.S.E. Collective, ‘Critical Approaches to Security in Europe: A Networked Manifesto’ (2006) 37 Security Dialogue 443 <https://journals.sagepub.com/doi/10.1177/0967010606073085> accessed 19 October 2021

Calabresi G, *The Cost of Accidents - A Legal and Economic Analysis* (Yale University Press 1970)

Campos F and others, ‘Assembly or Optimized C for Lightweight Cryptography on RISC-V?’ (2020) 12579 LNCS Lecture Notes in Computer Science 526 <https://link.springer.com/chapter/10.1007/978-3-030-65411-5_26> accessed 20 September 2021

Cardullo P and Kitchin R, ‘Smart Urbanism and Smart Citizenship: The Neoliberal Logic of “citizen-Focused” Smart Cities in Europe’ (2019) 37 Politics and Space 813

Casarin R and others, ‘Decision Trees and Random Forests’ in Mohammad Zoynul Abedin and others (eds), *The Essentials of Machine Learning in Finance and Accounting* (1st edn, Routledge, Taylor and Francis Inc 2021)

CEN - CENELEC, ‘CEN-CENELEC Response to the European Commission’ s Public Consultation on the Draft Machinery Regulation’ (2021) <https://www.cencenelec.eu/media/Policy Opinions/2021-07-07_cen-cenelecpositionondraftmachineryregulation.pdf>

Center for Strategy & Evaluation Services, ‘Final Report: Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment’ (2020) <https://ec.europa.eu/docsroom/documents/40763>

Chen K and others, ‘Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice’ (2018) 2 Journal of Hardware and Systems Security 97 <https://doi.org/10.1007/s41635-017-0029-7> accessed 17 September 2021

Cheruvu S and others, *Demystifying Internet of Things Security* (APRESS Open 2020)

Chiara PG, ‘Disentangling Encryption from the Personalization Debate: On the Advisability of Endorsing the “Relativist Approach” Underpinning the Identifiability Criterion’ (2020) 4 University of Vienna Law Review 168

——, ‘Sistemi Intelligenti Autonomi e Responsabilità Civile: Stato Dell’arte e Prospettive Nell’esperienza Comunitaria’ (2020) 1 Diritto ed Economia dell’Impresa 105

——, ‘The Balance Between Security, Privacy and Data Protection in IoT Data Sharing: A Critique to Traditional “Security&Privacy” Surveys’ (2021) 7 European Data Protection Law Review 18

——, ‘The IoT and the New EU Cybersecurity Regulatory Landscape’ (2022) 36 International Review of Law, Computers & Technology 118

Christofi A and others, ‘Erosion by Standardisation: Is ISO/IEC 29134:2017 on Privacy Impact Assessment up to (GDPR) Standard?’, *Research Anthology on Privatizing and Securing Data* (IGI Global 2021)

Christou G, ‘Introduction’, *Cybersecurity in the European Union* (Palgrave Macmillan UK 2016)

——, ‘Network and Information Security and Cyber Defence in the European Union’, *Cybersecurity in the European Union* (Palgrave Macmillan UK 2016)

CISCO, ‘The Internet of Everything - Global Public Sector Economic Analysis ’ (2013)

Citron D and Franks M, ‘Criminalizing Revenge Porn’ (2014) 49 Wake Forest Law Review <https://digitalcommons.law.umaryland.edu/fac_pubs/1420> accessed 2 October 2021

Clader A, *Nine Steps to Success: An ISO27001:2013 Implementation Overview* (Second, IT Governance Publishing 2013)

Clifford D and Ausloos J, ‘Data Protection and the Role of Fairness’ (2018) 37 Yearbook of European Law 130

CNIL, ‘PIA: Application to IoT Devices’ (2018) <https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual> accessed 31 January 2020

——, ‘Privacy Impact Assessment (PIA) Knowledge Bases’ (2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>

——, ‘Privacy Impact Assessment (PIA) Methodology’ (2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf>

——, ‘Privacy Impact Assessment (PIA) Templates’ (2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf>

——, ‘L’anonymisation de Données Personnelles ’ (2020) <https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles> accessed 5 May 2022

Cohen JE, ‘What Privacy Is For’ (2013) 126 Harvard Law Review 1904 <https://www.jstor.org/stable/23415061> accessed 7 October 2021

Cole MD, Etteldorf C and Ullrich C, *Cross-Border Dissemination of Online Content*, vol 81 (1st edn, Nomos Verlagsgesellschaft mbH & Co KG 2020) <https://doi.org/10.5771/9783748906438,> accessed 4 October 2021

Cole MD and Schmitz S, ‘The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape’ (2020) 017

Conley C, ‘Metadata: Piecing Together a Privacy Solution’ (2014) <https://www.aclunc.org/sites/default/files/Metadata report FINAL 2 21 14 cover %2B inside for web %283%29.pdf>

Contardi M, ‘Changes in the Medical Device’s Regulatory Framework and Its Impact on the Medical Device’s Industry: From the Medical Device Directives to the Medical Device Regulations’ (2019) 12 Erasmus Law Review 166

Cooter RD, ‘Economic Theories of Legal Liability’ (1991) 5 Journal of Economic Perspectives 11

Council of the European Union, ‘Preparation of the Council Position on the Evaluation and Review of the General Data Protection Regulation (GDPR) - Comments from Member States 12756/1/19 REV 1’ (2019) <https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf>

——, ‘Council Conclusions on ICT Supply Chain Security’, vol 13664/22 (2022) <https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf>

Cozzi E and others, ‘Understanding Linux Malware’ [2018] Proceedings - IEEE Symposium on Security and Privacy 161

D’Souza R and others, ‘Publicly Verifiable Secret Sharing for Cloud-Based Key Management’, *Progress in Cryptology – INDOCRYPT 2011* (Springer, Berlin, Heidelberg 2011) <https://link.springer.com/chapter/10.1007/978-3-642-25578-6_21> accessed 12 October 2021

Daskalova VI and Heldeweg MA, ‘Challenges for Responsible Certification in Institutional Context: The Case of Competition Law Enforcement in Markets with Certification’ in Peter Rott (ed), *Certification – Trust, Accountability, Liability* (Springer Cham 2019)

Data Protection Commission, ‘Guidance on Anonymisation and Pseudonymisation’ (2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614 Anonymisation and Pseudonymisation.pdf> accessed 5 May 2022

Davies D, ‘A Brief History of Cryptography’ (1997) 2 Information Security Technical Report 14

De Franceschi A and Lehmann M, ‘Data as Tradeable Commodity and New Measures for Their

Protection' (2015) 1 The Italian Law Journal 51

De Gregorio G and Dunn P, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59 Common Market Law Review 473

De Hert P and Gutwirth S, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006)

De Terwangne C, 'Article 5. Principle Relating to Processing of Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

——, 'Article 5. Principles Relating to Processing of Personal Data' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press 2020)

Denardis L, *The Internet in Everything - Freedom and Security in a World with No Off Switch*, vol 148 (1st edn, Yale University Press 2020)

Dickmann R, 'Vulnerability Management as Compliance Requirement in Product Security Regulation — a Game Changer for Producers ' Liability and Consequential Improvement of the Level of Security in the Internet of Things?' [2022] International Cybersecurity Law Review

DIGITALEUROPE, 'DIGITALEUROPE Position on the NIS2 Directive' (2021) <https://www.digitaleurope.org/resources/digitaleuropes-position-on-the-nis-2-directive/#:~:text=Finally%2C DIGITALEUROPE recommends that a,authorities in more Member States.>

——, 'DIGITALEUROPE Position Paper on the New Machinery Regulation' (2021)

——, 'Setting the Standard: How to Secure the Internet of Things' (2021) <https://www.digitaleurope.org/wp/wp-content/uploads/2021/07/DIGITALEUROPE_Joint-> accessed 18 October 2021

——, 'Building Blocks for a Scalable Cyber Resilience Act' (2022) <https://www.digitaleurope.org/wp/wp-content/uploads/2022/05/Building-blocks-for-a-scalable-Cyber-Resilience-Act.pdf>

——, 'DIGITALEUROPE Comments on the Proposed General Product Safety Regulation' (2022) <https://www.digitaleurope.org/resources/digitaleurope-comments-on-the-proposed-general-product-safety-regulation/>

——, 'Reporting, Mandatory Certification and Main Establishment in Final NIS2 Trilogues' (2022) <https://digital-europe-website-v1.s3.fr-

par.scw.cloud/uploads/2022/05/DIGITALEUROPE_Reporting-Mandatory-Certification-Main-Establishment-in-final-NIS2-trilogues.pdf>

Dooley JF, *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms* (Springer 2018)

Drexl J, 'Designing Competitive Markets for Industrial Data - Between Propertisation and Access' (2017) 8 JIPITEC 257 <http://www.ip.mpg.de/> accessed 19 April 2022

Ducuing C, 'Towards an Obligation to Secure Connected and Automated Vehicles "by Design"?', *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia 2019)

——, 'Understanding the Rule of Prevalence in the NIS Directive: C-ITS as a Case Study' (2021) 40 Computer Law and Security Review 105514 <https://doi.org/10.1016/j.clsr.2020.105514>

Durante M, *Ethics, Law and the Politics of Information: A Guide to the Philosophy of Luciano Floridi*, vol 18 (Springer Netherlands 2017) <http://link.springer.com/10.1007/978-94-024-1150-8> accessed 8 October 2021

——, 'Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks' in Don Berkich and Matteo Vincenzo D'Alfonso (eds), *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence*, vol 134 (Springer Nature 2019)

——, *Computational Power: The Impact of ICT on Law, Society and Knowledge* (Routledge 2021)

Dutta IK and others, 'Lightweight Polymorphic Encryption for the Data Associated with Constrained Internet of Things Devices', *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)* (IEEE 2020)

Dworkin MJ, 'SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions' (2015) <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf> accessed 10 May 2022

ECSO, 'European Cyber Security Certification - Challenges Ahead for the Roll-out of the Cybersecurity' <https://ecs-org.eu/documents/publications/5fd787e5cae1c.pdf>

EDPB, 'Opinion 5/2019 on the Interplay between the EPrivacy Directive and the GDPR, in Particular Regarding the Competence , Tasks and Powers of Data Protection Authorities' (2019)

——, 'Statement 03/2021 on the EPrivacy Regulation' (2021)

EDPB - EDPS, 'EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (2022) <https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf>

EDPS, ‘Opinion 9/2016 EDPS Opinion on Personal Information Management Systems: Towards More User Empowerment in Managing and Processing Personal Data’ (2016) <https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en>

——, ‘EDPS Opinion on Safeguards and Derogations under Article 89 GDPR in the Context of a Proposal for a Regulation on Integrated Farm Statistics ’ (2017) <https://edps.europa.eu/data-protection/our-work/publications/opinions/farm-statistics_en> accessed 1 June 2022

——, ‘EDPS Comments on a Framework for the Free-Flow of Non-Personal Data in the EU ’ (2018) <https://edps.europa.eu/data-protection/our-work/publications/comments/edps-comments-framework-free-flow-non-personal-data_en> accessed 3 June 2022

EDPS and AEPD, ‘Introduction to the Hash Function as a Personal Data Pseudonymisation Technique’ (2019) <https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf> accessed 26 February 2020

Edwards L, ‘Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective’ (2016) 2 European Data Protection Law Review <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/429125/future-cities-global-> accessed 16 March 2022

Egorov M, Wilkison M and David Nuñez N, ‘NuCypher KMS: Decentralized Key Management System’

Elliott D, ‘Data Protection Is More than Privacy’ (2019) 5 European Data Protection Law Review 13

ENISA, ‘Malicious Software - Train the Trainer Reference Guide’ (2010) <http://www.enisa.europa.eu/> accessed 20 September 2021

——, ‘Definition of Cybersecurity: Gaps and Overlaps in Standardisation’ (2015)

——, ‘Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics’ (2015) <https://www.enisa.europa.eu/publications/big-data-protection> accessed 18 February 2020

——, ‘ENISA’s Opinion Paper on Encryption - Strong Encryption Safeguards Our Digital Identity’ (2016) <www.enisa.europa.eu> accessed 8 October 2021

——, ‘A Tool on Privacy Enhancing Technologies (PETs) Knowledge Management and Maturity Assessment’ (2017)

——, ‘Ad-Hoc & Sensor Networking for M2M Communications Threat Landscape and Good Practice Guide’, vol 83 (2017) <https://www.enisa.europa.eu/publications/m2m-communications-

threat-landscape>

——, ‘Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures’ (2017) <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>

——, ‘ENISA Overview of Cybersecurity and Related Terminology Foreword by the Executive Director’ (2017)

——, ‘Handbook on Security of Personal Data Processing’ (2017) <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing>

——, ‘Incident Notification for DSPs in the Context of the NIS Directive - A Comprehensive Guideline on How to Implement Incident Notification for Digital Service Providers, in the Context of the NIS Directive’ (2017)

——, ‘Recommendations on Shaping Technology According to GDPR Provisions: An Overview on Data Pseudonymisation’ (2018)

——, ‘Recommendations on Shaping Technology According to GDPR Provisions’ (2018)

——, ‘Reference Incident Classification Taxonomy Task Force Status and Way Forward’ (2018)

——, ‘Public Private Partnerships (PPP) - Cooperative Models ’ (2018) <https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models> accessed 5 October 2021

——, ‘ENISA Threat Landscape for 5G Networks’ (2019)

——, ‘Good Practices for Security of IoT Secure Software Development Lifecycle’ (2019) <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1>

——, ‘IoT Security Standards Gap Analysis: Mapping of Existing Standards against Requirements on Security and Privacy in the Area of IoT’ (2019)

——, ‘Pseudonymisation Techniques and Best Practices: Recommendations on Shaping Technology According to Data Protection and Privacy Provisions’ (2019)

——, ‘Standardisation in Support of the Cybersecurity Certification: Recommendations for European Standardisation in Relation to the Cybersecurity Act’ (2019)

——, ‘Artificial Intelligence Threat Landscape Report ’ (2020) <https://www.enisa.europa.eu/news/enisa-news/enisa-ai-threat-landscape-report-unveils-major-cybersecurity-challenges> accessed 21 September 2021

——, ‘Encrypted Traffic Analysis: Use Cases & Security Challenges’ (2020) <https://www.enisa.europa.eu/publications/encrypted-traffic-analysis>

——, ‘ENISA Threat Landscape - Distributed Denial of Service’ (2020)

——, ‘ENISA Threat Landscape 2020 - Malware’ (2020) <https://www.enisa.europa.eu/publications/malware> accessed 20 September 2021

——, ‘ENISA Threat Landscape 2020 - Ransomware’ (2020) <https://www.enisa.europa.eu/publications/ransomware> accessed 20 September 2021

——, ‘ENISA Threat Landscape 2020 - Web Application Attacks’ (2020) <https://www.enisa.europa.eu/publications/web-application-attacks> accessed 20 September 2021

——, ‘EUCS - CLOUD SERVICES SCHEME: EUCS, a Candidate Cybersecurity Certification Scheme for Cloud Services’ (2020)

——, ‘Guidelines for Securing the Internet of Things - Secure Supply Chain for IoT’ (2020)

——, ‘The Year in Review ENISA Threat Landscape - From January 2019 to April 2020’ (2020) <https://www.thehaguesecuritydelta.com/media/com_hsd/report/337/document/ETL2020-A-year-in-review-A4-4-.pdf> accessed 2 October 2021

——, ‘Data Pseudonymisation Techniques: Advanced Techniques & Use Cases. Technical Analysis of Cybersecurity Measures in Data Protection and Privacy’ (2021)

——, ‘ENISA Threat Landscape 2021: April 2020 to Mid-July 2021’ (2021) <https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020>

——, ‘Cybersecurity Certification: Candidate EUCC Scheme V1.1.1’ (2021)

——, ‘Public Consultation on the Draft Candidate EUCC Scheme’ (2021)

——, ‘Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education’ (2021) <https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education> accessed 27 November 2021

——, ‘NIS Investments’ (2021) <https://www.enisa.europa.eu/publications/nis-investments-2021> accessed 27 November 2021

——, ‘Data Protection Engineering: From Theory to Practice’ (2022)

——, ‘Research and Innovation Brief: Annual Report on Cybersecurity Research and Innovation’ (2022) <https://www.enisa.europa.eu/publications/research-and-innovation-brief>

ENISA Stakeholder Cybersecurity Certification Group, ‘Consultation Report on Draft URWP’ (2021)

EPDS, ‘EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (EPrivacy Regulation)’ (2017) <https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf>

Ermakova T and Fabian B, ‘Secret Sharing for Health Data in Multi-Provider Clouds’ [2013] Proceedings - 2013 IEEE International Conference on Business Informatics, IEEE CBI 2013 93

Esayas SY, ‘The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules : Beyond the “all or Nothing” Approach’ (2015) 6 European Journal of Law and Technology 1

ETSI, ‘EN 303 645 V2.1.1 - Cyber Security for Consumer Internet of Things: Baseline Requirements’ (2020)

Etteldorf C, ‘A New Wind in the Sails of the EU Eprivacy-Regulation or Hot Air Only? On an Updated Input from the Council of the EU under German Presidency’ (2020) 6 European Data Protection Law Review 567

European Commission, ‘Shaping Europe’s Digital Future ’ <https://digital-strategy.ec.europa.eu/it> accessed 14 June 2022

——, ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions Network and Information Security: Proposal for A European Policy Approach’ (2001) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298>

——, ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions “I2010-A European Information Society for Growth and Employment” COM(2005) 229 Final’ (2005)

——, ‘Communication from the Commission of 31 May 2006: A Strategy for a Secure Information Society “Dialogue, Partnership and Empowerment” COM(2006) 251 Final’ (2006) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al24153a>

——, ‘Communication from the Commission on a European Programme for Critical Infrastructure Protection’ (2006) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN> accessed 24 November 2021

——, ‘Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) COM(2007) 228 Final’ (2007) <http://eurlex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf> accessed 9 May 2022

——, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from Large Scale Cyber-Attacks And ’ (2009) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF> accessed 24 November 2021

——, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe COM(2010) 245 Final’ (2010) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> accessed 24 November 2021

——, ‘Communication from the Commission to the European Parliament and the Council The EU Internal Security Strategy in Action: Five Steps towards a More Secure Europe COM(2010) 673 Final’ (2010) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF> accessed 24 November 2021

——, ‘Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 Final’ (2013) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN> accessed 24 November 2021

——, ‘COMMISSION STAFF WORKING DOCUMENT Part 1: Evaluation of the Internal Market Legislation for Industrial Products Accompanying the Document: The Communication from the Commission to the European Parliament, the Council and the European Economic and Social C’ (2014) <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52014SC0023> accessed 7 December 2021

——, ‘Public Consultation on the Public-Private Partnership on Cybersecurity and Possible Accompanying Measures | Shaping Europe’s Digital Future’ (2015) <https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-public-private-partnership-cybersecurity-and-possible-accompanying-measures> accessed 5 October 2021

——, ‘The “Blue Guide” on the Implementation of EU Products Rules 2016 (2016/C 272/01)’ [2016] Official Journal of the European Union <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016XC0726(02)&from=EN%0Ahttp://ec.europa.eu/DocsRoom/documents/18027/>

——, ‘ANNEX to the COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Making the Most of NIS – towards the Effective Implementation of Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Info’ (2017) <https://eur-lex.europa.eu/resource.html?uri=cellar:d829f91d-9859-11e7-b92d-01aa75ed71a1.0001.02/DOC_4&format=PDF>

——, ‘Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU’ (2017) <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017JC0450> accessed 30 November 2021

——, ‘State of the Union 2017 - Cybersecurity: EU Agency and Certification Framework’ (2017) <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193>

——, ‘Commission Staff Working Document - Liability for Emerging Digital Technologies - Accompanying the Document: Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and Th’ (2018)

——, ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Building Trust in Human-Centric Artificial Intelligence COM/2019/168 Final’ (2019) <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52019DC0168> accessed 12 October 2021

——, ‘Rolling Plan for ICT Standardisation 2019’ (2019)

——, ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS An SME Strategy for a Sustainable and Digital Europe COM(2020) 103 Final’ (2020)

——, ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy’ (2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605> accessed 6 October 2021

——, ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data Protection as a Pillar of Citizens’ Empowerment and the EU’s Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation COM/2020’ (2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> accessed 12 October 2021

——, ‘Recovery Plan for Europe ’ (2020) <https://ec.europa.eu/info/strategy/recovery-plan-europe_en> accessed 14 June 2022

——, ‘REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics

COM/2020/64 Final' (2020) <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064> accessed 12 October 2021

——, 'Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148 COM(2020) 823 Final' (2020) <https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF> accessed 28 October 2021

——, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Commission Delegated Regulation Supplementing Directive 2014/53/EU of the European Parliament and of the Council with Regard to the Application of the Essential Requireme' (2021) <https://ec.europa.eu/growth/system/files/2021-10/SWD%282021%29302_EN_impact_assessment_part1_v3.pdf>

——, 'Rolling Plan for ICT Standardisation 2021' (2021)

——, 'State of the Union 2021 - Letter of Intent' (2021) <https://ec.europa.eu/info/sites/default/files/state_of_the_union_2021_letter_of_intent_en.pdf>

European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade' (2020)

European Commission Expert Group on Liability and New Technologies, 'Liability for Artificial Intelligence and Other Emerging Digital Technologies' (2019)

European Commission High Level Group of Scientific Adivisors, 'Cybersecurity in the European Digital Single Market' (2017) <https://portal-cdn.scnat.ch/asset/ed5ae04c-1d2c-5c4f-a961-0b050fe0aa50/SAM_Cybersecurity_scientific_opinion.pdf?b=79e9c1e8-989d-5e60-a3b6-4d891f883626&v=346b7cdc-8d1b-56b5-b9b8-f270a609de88_0&s=E3AVFGsn1eZLAAjXDYG5mEbvy0RFNJHp7BK9RTe-k2WeglibkB5lzU41kidSWMNZfJlZ2zM_jwzYiPB90V-sErEZal-eqg5qbj7FWIoMhL1Uv1-HM1Osx_aKDys2tahJsdjTb7sLxNRqg3ItHewOUuBsAUnkPHs52BtJ3oGgo9E> accessed 8 October 2021

European Council, ' The Stockholm Programme - An Open and Secure Europe Serving and Protecting Citizens' (2010) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF> accessed 23 November 2021

European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights* (Council of Europe 2021)

European Data Protection Supervisor, 'Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive' (2021)

European Economic and Social Committee, 'Revision of the Machinery Directive ' (2021) <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/information-reports/revision-machinery-directive> accessed 6 June 2022

European Parliament, 'European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))' (2017) <https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf> accessed 18 October 2021

——, 'Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics' (2017)

EUROPOL, 'Internet Organised Crime Threat Assessment (IOCTA)' (2020) <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020> accessed 2 October 2021

Eurosmart, 'Cyber Resilience Act (CRA) - New Cybersecurity Rules for Digital Products and Ancillary Services' (2022) <https://www.eurosmart.com/cyber-resilience-act-cra-new-cybersecurity-rules-for-digital-products-and-ancillary-services/>

Fairgrieve D and others, 'Product Liability Directive' in Piotr Machnikowski (ed), *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (Intersentia 2017)

Fantin S, 'Weighting the EU Cybersecurity Act: Progress or Missed Opportunity? ' (2019) <https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS2783850&context=L&vid=Lirias&search_scope=Lirias&tab=default_tab&lang=en_US&fromSitemap=1> accessed 5 October 2021

Farkas TJ, 'Data Created by the Internet of Things: The New Gold without Ownership?' (2017) 23 Revista La Propiedad Inmaterial 5 <https://revistas.uexternado.edu.co/index.php/propin/article/view/4975/6065> accessed 19 April 2022

FDA, 'FDA Approves Pill with Sensor That Digitally Tracks If Patients Have Ingested Their Medication ' (2017) <https://www.fda.gov/news-events/press-announcements/fda-approves-pill-sensor-digitally-tracks-if-patients-have-ingested-their-medication> accessed 28 September 2021

Finck M and Pallas F, ‘They Who Must Not Be Identified — Distinguishing Personal from Non-Personal Data under the GDPR’ (2020) 10 International Data Privacy Law 11

Finnish Transport and Communications Agency, ‘Finnish Cybersecurity Label’ (2020) <https://tietoturvamerkki.fi/files/cybersecurity_label_presentation-280920.pdf>

Floridi L, ‘The Ontological Interpretation of Informational Privacy’ (2005) 7 Ethics and Information Technology 185

——, ‘Mature Information Societies-a Matter of Expectations’ (2016) 29 Philosophy & Technology 1

——, ‘On Human Dignity as a Foundation for the Right to Privacy’ (2016) 29 Philosophy & Technology 307 <https://link.springer.com/article/10.1007/s13347-016-0220-8> accessed 7 October 2021

——, ‘Infraethics–on the Conditions of Possibility of Morality’ (2017) 30 Philosophy & Technology 391 <https://link.springer.com/article/10.1007/s13347-017-0291-1> accessed 8 October 2021

——, ‘Soft Ethics and the Governance of the Digital’ (2018) 31 Philosophy & Technology 2018 31:1 1 <https://link.springer.com/article/10.1007/s13347-018-0303-9> accessed 20 September 2021

——, *Il Verde e Il Blu - Idee Ingenue per Migliorare La Politica* (Raffaello Cortina Editore 2020)

——, ‘The End of an Era: From Self-Regulation to Hard Law for the Digital Industry’ (2021) 34 Philosophy & Technology 619

Floridi L and Sideri M, ‘Piramide Onlife’ *Corriere Innovazione* (28 May 2021)

Floridi L and Strait A, ‘Ethical Foresight Analysis: What It Is and Why It Is Needed?’ (2020) 30 Minds and Machines 77 <https://link.springer.com/article/10.1007/s11023-020-09521-y> accessed 5 October 2021

Fosch-Villaronga E and Mahler T, ‘Cybersecurity, Safety and Robots: Strengthening the Link between Cybersecurity and Safety in the Context of Care Robots’ (2021) 41 Computer Law & Security Review

Friedewald M and others, ‘Data Protection Impact Assessments in Practice: Experiences from Case Studies’, *ESORICS 2021: Computer Security. ESORICS 2021 International Workshops*, vol 13106 LNCS (Springer International Publishing 2022)

Fuster GG and Hijmans Hielke, ‘The EU Rights to Privacy and Personal Data Protection: 20 Years in 10 Questions - Discussion Paper’, *International Workshop ‘Exploring the Privacy and Data Protection connection: International Workshop on the Legal Notions of Privacy and Data*

Protection in EU Law in a Rapidly Changing World' (2019) <https://brusselsprivacyhub.eu/events/20190513.Working_Paper_González_Fuster_Hijmans.pdf> accessed 31 January 2020

Fuster GG and Jasmontaite L, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer, Cham 2020) <https://link.springer.com/chapter/10.1007/978-3-030-29053-5_5> accessed 2 October 2021

Fuster GG, Van Brakel R and De Hert P, 'Co-Regulation and Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and Data Protection-by-Design' in Gloria González Fuster, Rosamunde van Brakel and Paul De Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar Publishing 2022)

Garante per la Protezione dei Dati Personali, 'Guidelines on the Use of Cookies and Other Tracking Tools - 10 June 2021' (2021) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876>

Gellert R, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016) 2 European Data Protection Law Review 481

Gellert R, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279

——, 'Personal Data's Ever-Expanding Scope in Smart Environments and Possible Path(s) for Regulating Emerging Digital Technologies' (2021) 11 International Data Privacy Law 196

Gérardy M, 'Nemo Censetur Ignorare Legem: The Dilemma Regarding the Access to ISO Standards Referenced into EU Law' (*REALaw.blog*) <https://realaw.blog/2021/11/23/nemo-censetur-ignorare-lege-the-dilemma-regarding-the-access-to-iso-standards-referenced-into-eu-law-by-marie-gerardy/> accessed 7 December 2021

German Federal Office for Information Security (BSI), 'IT Security Label for All "Smart Consumer Devices"' (2022) <https://www.bsi.bund.de/SharedDocs/IT-Sicherheitskennzeichen/DE/Meldungen/Smarte-Verbrauchergeraete.html>

Gerybaite A, 'Exploring the Regulatory Interplay in Health Internet of Everything: Digital Health Technologies, Data Protection and Cybersecurity' [2022] Forthcoming 1

Giffinger R and others, 'Smart Cities-Ranking of European Medium-Sized Cities' (2007) <http://www.smart-cities.eu> accessed 22 September 2021

Gijrath SJH, '(Re-)Defining Software Defined Networks under the European Electronic Communications Code' (2021) 40 Computer Law & Security Review

Giovanni C and Silva F, 'Cybersecurity for Connected Products - ANEC BEUC Position Paper' (2018)

Gkotsopoulou O and others, 'Data Protection by Design for Cybersecurity Systems in a Smart Home Environment' [2019] Proceedings of the 2019 IEEE Conference on Network Softwarization: Unleashing the Power of Network Softwarization, NetSoft 2019 101

González EG, Hert P De and Papakonstantinou V, 'The Proposed EPrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads?' in Dara Hallinan and others (eds), *Data Protection and Privacy: Data Protection and Democracy* (Hart Publishing 2020)

Gorywoda L, 'The New European Legislative Framework for the Marketing of Goods' (2009) 16 Columbia Journal of European Law 161

Graef I and others, 'Feedback to the Commission's Proposal on a Framework for the Free Flow of Non-Personal Data' [2018] SSRN Electronic Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3106791> accessed 17 February 2020

Graef I, Gellert R and Husovec M, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation' (2020) 44 European Law Review 605

Graef I and Husovec M, 'Seven Things to Improve in the Data Act' [2022] SSRN Electronic Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793>

Grotto AJ and Schallbruch M, 'Cybersecurity and the Risk Governance Triangle' (2021) 2 International Cybersecurity Law Review 77 <https://link.springer.com/article/10.1365/s43439-021-00016-9> accessed 4 November 2021

GSMA, 'Consultation on the Revision of the NIS Directive' (2020) <https://www.gsma.com/gsmaeurope/wp-content/uploads/2020/10/GSMA-Response-to-EC-public-consultation-on-NIS-Review.pdf> accessed 3 December 2021

Guttman B and Roback E, *An Introduction to Computer Security: The NIST Handbook, Special Publication (NIST SP)* (1995) <https://doi.org/10.6028/NIST.SP.800-12r1>

Gutwirth S and De Hert P, 'Regulating Profiling in a Democratic Constitutional State' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008)

Hadzovic S, 'Internet of Things from a Regulatory Point of View', *20th International Symposium INFOTEH-JAHORINA (INFOTEH)* (Institute of Electrical and Electronics Engineers Inc 2021)

Halevi S, ‘Homomorphic Encryption’ in Yehuda Lindell (ed), *Tutorials on the Foundations of Cryptography* (Springer International Publishing 2017)

Hallinan D and Martin N, ‘Fundamental Rights, the Normative Keystone of DPIA’ (2020) 6 European Data Protection Law Review 178

Halperin D and others, ‘Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses’, *2008 IEEE Symposium on Security and Privacy* (IEEE 2008)

Hatto P, ‘Standards and Standardization Handbook’ (2010) <http://www.nanostair.eu-vri.eu/filehandler.ashx?file=12450>

Hegarty R and Haggerty J, ‘Presence Metadata in the Internet of Things: Challenges and Opportunities’, *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)* (2020)

Heinz C and others, ‘Privacy, GDPR, and Homomorphic Encryption’ in Carna Zivkovic, Yajuan Guan and Christoph Grimm (eds), *IoT Platforms, Use Cases, Privacy, and Business Models: With Hands-on Examples Based on the VICINITY Platform* (Springer Nature 2021)

Helminger L and Rechberger C, ‘Multi-Party Computation in the GDPR’, *Privacy Symposium 2022 - Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT)* (2022)

Hernandez-Ramos JL and others, ‘Toward a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data-Protection Policies’ (2020) 18 IEEE Security and Privacy 28

Hernandez-Ramos JL, Matheu SN and Skarmeta A, ‘The Challenges of Software Cybersecurity Certification’ (2021) 19 IEEE Security and Privacy 99

Herrmann D and Pridöhl H, ‘Basic Concepts and Models of Cybersecurity’ in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer Science and Business Media BV 2020)

Hessel S and Rebmann A, ‘Regulation of Internet-of-Things Cybersecurity in Europe and Germany as Exemplified by Devices for Children’ (2020) 1 International Cybersecurity Law Review 27 <https://link.springer.com/article/10.1365/s43439-020-00006-3> accessed 4 November 2021

Hewlett Packard, ‘HP News - HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack’ (2014) <https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676>

Hildebrandt M, ‘Digital Security and Human Rights: A Plea for Counter-Infringement Measures’ in Mart Susi (ed), *Human Rights, Digital Society and the Law* (1st edn, Routledge 2019)

Ho Derek Leung Pratyush Mishra Ashkan Hosseini Dawn Song David Wagner G and others, 'Smart Locks: Lessons for Securing Commodity Internet of Things Devices' (2016) <http://www.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-11.html> accessed 14 October 2021

Hobbes T, *Leviathan [1651]* (Richard Tuck ed, Cambridge University Press 1996)

Hofmann HCH, 'European Regulatory Union? The Role of Agencies and Standards'' in Panos Koutrakos and Jukka Snell (eds), *Research Handbook on the EU's Internal Market* (Elgar Publishing 2016)

Hogan Lovells, 'A Comparison of IoT Regulatory Uncertainty in the EU China and the United States' (2019) <https://www.hlmediacomms.com/files/2019/03/Hogan-Lovells-A-comparison-of-IoT-regulatory-uncertainty-in-the-EU-China-and-the-United-States-March-2019.pdf>

Horkheimer M, *Critical Theory: Selected Essays* (Matthew O'Connell (translated by) ed, The Continuum Publishing Company 2002) <https://monoskop.org/images/7/74/Horkheimer_Max_Critical_Theory_Selected_Essays_2002.pdf> accessed 19 October 2021

Horkheimer M and Adorno TW, *Dialectic of Enlightenment: Philosophical Fragments* (Gunzelin Schmid Noerr and Edmund Jephcott (translated by) eds, Stanford University Press 2002)

Humayun M and others, 'Internet of Things and Ransomware: Evolution, Mitigation and Prevention' (2021) 22 Egyptian Informatics Journal 105

Hummel P, Braun M and Dabrock P, 'Own Data? Ethical Reflections on Data Ownership' (2021) 34 Philosophy and Technology 545

Iannacci J, 'Internet of Things (IoT); Internet of Everything (IoE); Tactile Internet; 5G – A (Not so Evanescent) Unifying Vision Empowered by EH-MEMS (Energy Harvesting MEMS) and RF-MEMS (Radio Frequency MEMS)' (2018) 272 Sensors and Actuators, A: Physical 187 <http://dx.doi.org/10.1016/j.sna.2018.01.038>

Information Commissioner's Office, 'Anonymisation: Managing Data Protection Risk Code of Practice' (2012) <https://ico.org.uk/media/1061/anonymisation-code.pdf> accessed 6 May 2022

——, 'Introduction to Anonymisation' (2021) <https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf> accessed 6 May 2022

Ioannidou I and Sklavos N, 'On General Data Protection Regulation Vulnerabilities and Privacy Issues , for Wearable Devices and Fitness Tracking Applications' (2021) 5 Cryptography

Iorga M and others, 'Fog Computing Conceptual Model' (2018) <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf> accessed 20

September 2021

Islam N and others, 'A Review of Applications and Communication Technologies for Internet of Things (IoT) and Unmanned Aerial Vehicle (UAV) Based Sustainable Smart Farming' (2021) 13 Sustainability 1821 <https://www.mdpi.com/2071-1050/13/4/1821/htm> accessed 21 September 2021

Ismail T and others, 'Hybrid and Secure E-Health Data Sharing Architecture in Multi-Clouds Environment', *ICOST 2020: The Impact of Digital Technologies on Public Health in Developed and Developing Countries*, vol 12157 LNCS (Springer, Cham 2020) <https://link.springer.com/chapter/10.1007/978-3-030-51517-1_21> accessed 12 October 2021

ISO/IEC, 'ISO/IEC 30141:2016 Information Technology-Internet of Things Reference Architecture (IoT RA) CD Stage' (2016) <www.iso.org> accessed 22 September 2021

——, 'ISO/IEC 30141:2018(En), Internet of Things (LoT) — Reference Architecture' (2018) <https://www.iso.org/obp/ui/es/#iso:std:iso-iec:30141:ed-1:v1:en> accessed 20 September 2021

ITU-T, 'Overview of the Internet of Things', vol 6 (2012)

Jabri V, 'Security: Critique, Analysis and Ethics' in Jonna Nyman and Anthony Burke (eds), *Ethical security studies : a new research agenda* (Routledge 2016)

Janeček V, 'Ownership of Personal Data in the Internet of Things' (2018) 34 Computer Law & Security Review 1039

Janssen A, 'The Update Obligation for Smart Products – Time Period for the Update Obligation and Failure to Install the Update' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Smart Products: Münster Colloquia on EU Law and the Digital Economy VI* (Nomos Verlag 2022)

Jorgensen P, *Applied Cryptography: Protocols, Algorithm, and Source Code in C*, vol 13 (Wiley Inc 1996)

Kamara I, 'Misaligned Union Laws? A Comparative Analysis of Certification in the Cybersecurity Act and the General Data Protection Regulation' in Dara Hallinan, Ronald Leenes and Paul De Hert (eds), *Data protection and Privacy: Data Protection and Artificial intelligence* (Hart Publishing 2021)

Katz J and Lindell Y, *Introduction to Modern Cryptography*, vol 6 (CRC Press Taylor & Francis Group 2015)

Kerber W, 'Governance of IoT Data: Why the EU Data Act Will Not Fulfill Its Objectives' [2022] SSRN Electronic Journal <https://papers.ssrn.com/abstract=4080436> accessed 12 July 2022

Kilovaty I, 'An Extraterritorial Human Right to Cybersecurity' (2020) 10 Notre Dame Journal of

International & Comparative Law 35

Klimas T, ‘The Law of Recitals in European Community Legislation’ (2008) 15 ILSA Journal of International & Comparative Law 61

Kohler C, ‘The EU Cybersecurity Act and European Standards: An Introduction to the Role of European Standardization’ (2020) 1 International Cybersecurity Law Review 7 <https://link.springer.com/article/10.1365/s43439-020-00008-1> accessed 4 November 2021

Kokott J and Sobotta C, ‘The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR’ (2013) 3 International Data Privacy Law 222

Kolcun R and others, ‘Revisiting IoT Device Identification’, *Network Traffic Measurement and Analysis Conference (TMA)* (2021) <https://arxiv.org/pdf/2107.07818.pdf> accessed 11 May 2022

Koolen C, ‘Transparency and Consent in Data-Driven Smart Environments’ (2021) 7 European Data Protection Law Review 174

Koops B-J, ‘On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy’ (2014) 3 Politica e Società 247

Koops B and others, ‘A Typology of Privacy’ (2017) 38 University of Pennsylvania Journal of International Law 483

Koops BJ and Kosta E, ‘Looking for Some Light through the Lens of “Cryptowar” History: Policy Options for Law Enforcement Authorities against “Going Dark”’ (2018) 34 Computer Law & Security Review 890

Kosta E, *Consent in European Data Protection Law*, vol 3 (Fabian Amtenbrink and Ramses A Wessel eds, Martinus Nijhoff Publishers 2013)

——, ‘Article 35 Data Protection Impact Assessment’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

——, ‘Article 7 Conditions for Consent’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Kotschy W, ‘Article 6 Lawfulness of Processing’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press 2020)

Kounoudes AD and Kapitsaki GM, ‘A Mapping of IoT User-Centric Privacy Preserving Approaches to the GDPR’ (2020) 11 Internet of Things

Kuan Hon W, Millard C and Walden I, ‘The Problem of “Personal Data” in Cloud Computing: What Information Is Regulated?—The Cloud of Unknowing’ (2011) 1 International Data Privacy Law 211

Kuner C, *European Data Protection Law : Corporate Compliance and Regulation* (Oxford University Press 2007)

Lachaud E, 'ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification' (2020) 6 European Data Protection Law Review 194

Lai CS and others, 'A Review of Technical Standards for Smart Cities' (2020) 2 Clean Technologies 290 <https://www.mdpi.com/2571-8797/2/3/19/htm> accessed 22 September 2021

Lancelot JF, 'Cyber-Diplomacy: Cyberwarfare and the Rules of Engagement' (2020) 4 Journal of Cyber Security Technology 240 <https://www.tandfonline.com/doi/abs/10.1080/23742917.2020.1798155> accessed 2 October 2021

Laud P and others, 'Basic Constructions of Secure Multiparty Computation' in Peeter Laud and Liina Kamm (eds), *Application of Secure Multiparty Computation* (IOS Press 2015)

Leese M, Lidén K and Nikolova B, 'Putting Critique to Work: Ethics in EU Security Research' (2019) 50 Security Dialogue 59 <https://doi.org/10.1177/0967010618809554>

Lock T, 'Article 10 CFR: Freedom of Thought, Conscience and Religion' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press 2019)

——, 'Article 14 CFR: Right to Education' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press 2019)

——, 'Article 3 CFR: Right to the Integrity of the Person' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press 2019)

Locke J, *Two Treatises of Government [1690]* (Peter Laslett ed, Cambridge University Press 1967) <https://books.google.com/books/about/Locke_Two_Treatises_of_Government.html?hl=it&id=5FziTdwA6WAC> accessed 14 October 2021

Loi M and Christen M, 'Ethical Frameworks for Cybersecurity' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer Science and Business Media BV 2020)

Loideain NN, 'A Port in the Data-Sharing Storm: The GDPR and the Internet of Things' (2019) 4 Journal of Cyber Policy 178 <https://www.tandfonline.com/doi/abs/10.1080/23738871.2019.1635176> accessed 8 October 2021

Lundevall-unger P and Tranvik T, 'IP Addresses – Just a Number?' (2011) 19 International Journal of Law and Information Technology 53

Lupton D, ‘M-Health and Health Promotion: The Digital Cyborg and Surveillance Society’ (2012) 10 Social Theory & Health 2012 10:3 229 <https://link.springer.com/article/10.1057/sth.2012.6> accessed 21 September 2021

Lynskey O, ‘Deconstructing Data Protection: The “added-Value” of a Right to Data Protection in the Eu Legal Order’ (2014) 63 International and Comparative Law Quarterly 569

——, *The Foundations of EU Data Protection Law* (Oxford University Press 2015)

Malgieri G, ‘Property and (Intellectual) Ownership of Consumers’ Information: A New Taxonomy for Personal Data ’ (2016) 4 Privacy in Germany 133 <https://researchportal.vub.be/en/publications/property-and-intellectual-ownership-of-consumers-information-a-ne> accessed 19 April 2022

Mandalari AM and others, ‘Towards Automatic Identification and Blocking of Non-Critical IoT Traffic Destinations’ (2020) <http://arxiv.org/abs/2003.07133>

Manky D, ‘Cybercrime as a Service: A Very Modern Business’ (2013) 2013 Computer Fraud & Security 9

Mansfield-Devine S, ‘Weaponising the Internet of Things’ (2017) 2017 Network Security 13

Mantelero A, ‘Comment to Articles 35 and 36’ in Mark D Cole and Franziska Boehm (eds), *GDPR Commentary* (Edward Elgar Publishing) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362747>

——, ‘From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy* (Springer 2017)

——, ‘AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment’ (2018) 34 Computer Law & Security Review 754

——, ‘The Future of Data Protection: Gold Standard vs. Global Standard’ (2021) 40 Computer Law & Security Review 105500

——, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (Springer 2022)

——, ‘The Common EU Approach to Personal Data and Cybersecurity Regulation’ (2021) 28 International Journal of Law and Information Technology 297 <https://academic.oup.com/ijlit/article/28/4/297/6120059> accessed 4 October 2021

Markopoulou D, Papakonstantinou V and de Hert P, ‘The New EU Cybersecurity Framework: The NIS Directive, ENISA’s Role and the General Data Protection Regulation’ (2019) 35 Computer Law and Security Review 105336 <https://doi.org/10.1016/j.clsr.2019.06.007>

Martìn-Casals M, ‘Causation and Scope of Liability in the Internet of Things (IoT)’ in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things - Münster Colloquia on EU Law and the Digital Economy IV* (Bloomsbury Publishing 2019)

Martino L and Cappelletti F, ‘Achieving Robust European Cybersecurity through Public-Private Partnerships: Approaches and Developments Content’ (2021) 4 European Liberal Forum (ELF) <www.liberalforum.eu> accessed 5 October 2021

Martoni M, ‘Datificazione Dei Nativi Digitali e Società Della Classificazione. Prime Riflessioni Sull’educazione Alla Cittadinanza Digitale’ (2020) 1 Federalismi.it 119 <https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=40849> accessed 2 October 2021

Marwedel P, *Embedded System Design: Embedded Systems Foundations Of_Cyber-Physical Systems, and The_Internet Of_Things* (Fourth, Springer 2021)

Mcnutt P, ‘Public Goods and Club Goods’ (1999) 1 Encyclopedia of law and economics 927

Medical Device Coordination Group, ‘Guidance on Cybersecurity in Medical Devices’ (2019) <https://ec.europa.eu/docsroom/documents/41863>

Megas KN, Fagan M and Lemire D, ‘Workshop Summary Report for “Building the Federal Profile for IoT Device Cybersecurity” Virtual Workshop NISTIR 8322’ (2021) <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8322.pdf> accessed 20 September 2021

Meyer J, ‘The next Big Cyberthreat Isn’t Ransomware. It’s Killware. And It’s Just as Bad as It Sounds’ *USA Today* (12 October 2021) <https://eu.usatoday.com/story/news/politics/2021/10/12/cybersecurity-experts-warn-killware-attacks-rival-ransomware/6042745001/> accessed 18 October 2021

Ministry of Foreign Affairs of Italy, ‘Italian Position Paper on “International Law and Cyberspace”’ (2021) <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf>

Mitrou L, ‘Communications Data Retention: A Pandora’s Box for Rights and Liberties?’ in Alessandro Acquisti and others (eds), *Digital Privacy: Theory, Technologies, and Practices* (Auerbach Publications 2007)

Mittelstadt BD and others, ‘The Ethics of Algorithms: Mapping the Debate’ (2016) 3 Big Data and Society 205395171667967 <http://journals.sagepub.com/doi/10.1177/2053951716679679> accessed 31 March 2020

Mourby M and others, ‘Are “Pseudonymised” Data Always Personal Data? Implications of the

GDPR for Administrative Data Research in the UK' (2018) 34 Computer Law and Security Review 222

Mulligan DK and Schneider FB, 'Doctrine for Cybersecurity' (2011) 140 Daedalus 70

Narayanan A and Shmatikov V, 'Robust De-Anonymization of Large Sparse Datasets', *Proceedings - IEEE Symposium on Security and Privacy* (2008)

National Research Council, *Expanding the Vision of Sensor Materials* (National Academies Press 1995)

Nativi S, Kotsev A and Scudo P, *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins) A Multi-Facets Analysis* (Publications Office of the European Union 2020) <https://ec.europa.eu/jrc> accessed 20 September 2021

Nieles M, Dempsey K and Pillitteri VY, 'NIST Special Publication 800-12 Revision 1 - An Introduction to Information Security' (2017) <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf> accessed 31 January 2020

NIS Cooperation Group, 'Synergies in Cybersecurity Incident Reporting - CG Publication 04/20' (2020) <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>

NIST, 'Lightweight Cryptography | CSRC' <https://csrc.nist.gov/Projects/lightweight-cryptography> accessed 20 September 2021

——, 'Guide to Storage Encryption Technologies for End User Devices: Recommendations of the National Institute of Standards and Technology' (2007) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf>

——, 'NISTIR 8074 - Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity', vol 2 (Michael Hogan and Elaine Newton eds, 2015) <http://dx.doi.org/10.6028/NIST.IR.8074v2> accessed 4 October 2021

——, 'Framework for Cyber-Physical Systems Release 1.0' (2016)

——, 'Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1' (2018) <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> accessed 4 October 2021

Nolan A, 'Cybersecurity and Information Sharing: Legal Challenges and Solutions' (2015) <www.crs.gov> accessed 5 October 2021

Noto La Diega G, *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies* (Routledge, Taylor and Francis Inc 2023)

Odermatt J, ‘The European Union as a Cybersecurity Actor’ in Steven Blockmans and Panos Koutrakos (eds), *Research Handbook on EU Common Foreign and Security Policy* (Edward Elgar Publishing 2018)

Ohm P, ‘Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization’ (2009) 57 UCLA l. Rev. 1701

Omitola T and Wills G, ‘Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain’ (2018) 126 Procedia Computer Science 441

Orgalim, ‘Proposal for a Horizontal Legislation on Cybersecurity for Networkable Products within the New Legislative Framework’ (2020) <https://orgalim.eu/sites/default/files/attachment/Proposal for a horizontal legislation on cybersecurity for networkable products within the New Legislative Framework 091120 %28003%29.pdf> accessed 26 January 2022

——, ‘Orgalim Position on the Proposal for a General Product Safety Regulation’ (2021) <https://orgalim.eu/position-papers/internal-market-orgalim-position-proposal-general-product-safety-regulation>

Pa YMP and others, ‘IoTPOT: Analysing the Rise of IoT Compromises’, *WOOT ’15* (2015)

Pagallo U, *The Laws of Robots: Crimes, Contracts, and Torts* (Springer 2013)

——, ‘The Group, the Private, and the Individual: A New Level of Data Protection?’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy* (Springer 2017)

——, ‘The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection’ (2017) 3 European Data Protection Law Review 36

Pagallo U, Casanovas P and Madelin R, ‘The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data’ (2019) 7 Theory and Practice of Legislation 1

——, ‘The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data’ (2019) 7 Theory and Practice of Legislation 1

Pagallo U, Durante M and Monteleone S, ‘What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT’, *Data protection and privacy: (in)visibilities and infrastructures* (Springer, Cham 2017)

Palmirani M and Martoni M, ‘Big Data, Governance Dei Dati e Nuove Vulnerabilità’ (2019) 35 Notizie di Politeia 9

Panchenko A and others, ‘Website Fingerprinting at Internet Scale’, *NDSS* (2016)

Papakonstantinou V, ‘Cybersecurity as Praxis and as a State: The EU Law Path towards

Acknowledgement of a New Right to Cybersecurity?' (2022) 44 Computer Law and Security Review

Patringenaru I, 'A New Neuromorphic Chip for AI on the Edge, at a Small Fraction of the Energy and Size' (*UC San Diego News Center,* 17 August 2022) <https://ucsdnews.ucsd.edu/pressrelease/Nature_bioengineering_2022> accessed 29 August 2022

Paulsen C and Byers R, *Glossary of Key Information Security Terms, NIST Interagency/Internal Report (NISTIR)* (National Institute of Standards and Technology 2019) <https://doi.org/10.6028/NIST.IR.7298r3> accessed 2 October 2021

Perotto G, 'La Standardizzazione Europea Nel Settore Dell'ICT Nell'era Dell'Internet of Things: Qualificazione Giuridica e Controllo Di Validità Degli Standard Tecnici Armonizzati ' (2020) 3 Il diritto dell'economia 757

Pittoli P, David P and Noël T, 'Security Architectures in Constrained Environments: A Survey' (2018) 79 Ad Hoc Networks 112 <https://doi.org/10.1016/j.adhoc.2018.06.001>

Podda E and Palmirani M, 'Inferring the Meaning of Non-Personal, Anonymized, and Anonymous Data' in Victor Rodrìguez-Doncel and others (eds), *AI Approaches to the Complexity of Legal Systems XI-XII. AICOL AICOL XAILA 2020 2018 2020* (Springer International Publishing 2021)

Podda E and Vigna F, 'Anonymization Between Minimization and Erasure: The Perspectives of French and Italian Data Protection Authorities' in Andrea Kö and others (eds), *Electronic Government and the Information Systems Perspective: 10th International Conference, EGOVIS 2021* (Springer International Publishing 2021) <http://dx.doi.org/10.1007/978-3-030-86611-2_8>

Polčák R, 'Article 12. Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subject' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Poletti D, 'IoT and Privacy' in Roberto Senigaglia, Claudia Irti and Alessandro Bernes (eds), *Privacy and Data Protection in Software Services* (Springer 2022)

Prainsack B, 'Logged out: Ownership, Exclusion and Public Value in the Digital Data and Information Commons' (2019) 6 Big Data & Society

Pupillo L, 'EU Cybersecurity and the Paradox of Progress ' (2018) <https://www.ceps.eu/ceps-publications/eu-cybersecurity-and-paradox-progress/> accessed 5 October 2021

Purtova N, 'Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatization, and Ambient Intelligence' in Serge Gutwirth and others (eds), *Computers, Privacy and Data Protection: An Element of Choice* (Springer 2011) <https://research.tilburguniversity.edu/en/publications/property-in-personal-data-second-life-of-an-

old-idea-in-the-age-o> accessed 19 April 2022

——, *Property Rights in Personal Data: A European Perspective* (Wolters Kluwer Law International 2012)

——, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40

Quelle C, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502

Quinn P, 'The EU Commission's Risky Choice for a Non-Risk Based Strategy on Assessment of Medical Devices' (2017) 33 Computer Law & Security Review 361

Raab CD, 'Information Privacy, Impact Assessment, and the Place of Ethics' (2020) 37 Computer Law & Security Review 105404

Railean A and Reinhardt D, 'Let There Be Lite: Design and Evaluation of a Label for IoT Transparency Enhancement', *MobileHCI 2018 - Beyond Mobile: The Next 20 Years - 20th International Conference on Human-Computer Interaction with Mobile Devices and Services, Conference Proceedings Adjunct* (2018)

——, 'OnLITE: On-Line Label for IoT Transparency Enhancement' in Mikael Asplund and Simin Nadjm-Tehrani (eds), *Secure IT Systems - 25th Nordic Conference (NordSec 2020)* (Springer International Publishing 2021) <http://dx.doi.org/10.1007/978-3-030-70852-8_14>

Rak R, 'Internet of Healthcare: Opportunities and Legal Challenges in Internet of Things-Enabled Telehealth Ecosystems' [2021] 14th International Conference on Theory and Practice of Electronic Governance (ICEGOV) 481 <https://doi.org/10.1145/3494193.3494260> accessed 19 September 2022

Rao A and others, 'Probabilistic Threat Detection for Risk Management in Cyber-Physical Medical Systems' (2017) 35 IEEE Software 38

Rayes A and Salam S, *Internet of Things From Hype to Reality* (Springer 2019)

Reindl A and others, 'Legal and Technical Considerations on Unified, Safe and Data-Protected Haptic Telepresence in Healthcare' [2021] Proceedings of the 2021 IEEE International Conference on Intelligence and Safety for Robotics 239

Ren J and others, 'Information Exposure from Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach' [2019] Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC 267

Rizvi S and others, ‘Securing the Internet of Things (IoT): A Security Taxonomy for IoT’ [2018] Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018 163

——, ‘Threat Model for Securing Internet of Things (IoT) Network at Device-Level’ (2020) 11 Internet of Things 100240

ROBOLAW, ‘Final Report Summary - Regulating Emerging Robotic Technologies in Europe: Robotics Facing Law and Ethics’ (2014) <https://cordis.europa.eu/project/id/289092/reporting> accessed 22 November 2021

Rodotà S, ‘Privacy, Libertà, Dignità - Privacy, Freedom, and Dignity’, *Conclusive Remarks at the 26th International Conference on Privacy and Data Protection* (2004) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293> accessed 6 October 2021

Rodriguez AQ and others, ‘D2.3 ANASTACIA: Privacy Risk Modelling and Contingency Initial Report’ (2018) <www.ANASTACIA-h2020.eu> accessed 29 August 2022

Rosenzweig P, ‘Cybersecurity and Public Goods The Public/Private “Partnership”’ [2011] Emerging Threats in National Security and Law - Hoover Institution, Stanford University <https://www.hoover.org/sites/default/files/research/docs/emergingthreats_rosenzweig.pdf> accessed 5 October 2021

Rosner G and Kenneally E, ‘Privacy and the Internet of Things: Emerging Frameworks for Policy and Design’, *Berkeley Center for Long-Term Cybersecurity (CLTC) White Paper Series* (2018)

Rugge F, ‘Mind Hacking: La Guerra Informativa Nell’era Cyber’ (2018) 34 Notizie di Politeia 108

Sartor G and Omicini A, ‘The Autonomy of Technological Systems and Responsibilities for Their Use’ in Nehal Bhuta and others (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press 2016)

Schaffer SM, Schaffer DR and Colson DG, ‘A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults ’ (2020) 3 International Journal of Cybersecurity Intelligence & Cybercrime <https://www.doi.org/10.52306/03010420GXUV5876> accessed 5 October 2021

Schermer BW, ‘The Limits of Privacy in Automated Profiling and Data Mining’ (2011) 27 Computer Law and Security Review 45

Schiffner S and others, ‘Towards a Roadmap for Privacy Technologies and the General Data Protection Regulation: A Transatlantic Initiative’ in Manel Medina and others (eds), *Annual*

Privacy Forum 2018: Privacy Technologies and Policy (Springer, Cham 2018)

Schmitz-berndt S and Chiara PG, 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive' [2022] International Cybersecurity Law Review

Schmitz-Berndt S, 'Cybersecurity Is Gaining Momentum - NIS 2.0 Is on Its Way' (2021) 7 European Data Protection Law 580 <https://www.fnr.lu/projects/> accessed 23 February 2022

Schmitz-Berndt S and Anheier F, 'Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context' (2021) 7 European Data Protection Law Review 101 <https://edpl.lexxion.eu/data/article/16999/pdf/edpl_2021_01-014.pdf> accessed 26 October 2021

Schmitz-Berndt S and Schiffner S, 'Don't Tell Them Now (or at All)–Responsible Disclosure of Security Incidents under NIS Directive and GDPR' (2021) 35 International Review of Law, Computers and Technology 101 <https://doi.org/10.1080/13600869.2021.1885103>

Schmitz S and Schiffner S, 'Responsible Vulnerability Disclosure under the NIS 2.0 Proposal' (2021) 12 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 448 <https://www.jipitec.eu/issues/jipitec-12-5-2021/5495>

Schulz W and Hoboken J van, 'Human Rights and Encryption ' [2016] UNESCO Series on Internet Freedom <https://unesdoc.unesco.org/ark:/48223/pf0000246527?1=null&queryId=e05fdd78-68b9-4ff3-b7ce-b998b0c0cf01> accessed 3 June 2022

Schwab K, 'The Fourth Industrial Revolution: What It Means and How to Respond | World Economic Forum' (2016) <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> accessed 28 September 2021

Sehgal A and others, 'Management of Resource Constrained Devices in the Internet of Things' (2012) 50 IEEE Communications Magazine 144

Serpanos D and Wolf M, *Internet-of-Things (IoT) Systems - Architectures, Algorithms, Methodologies* (Springer International Publishing 2018)

Shackelford SJ, 'Should Cybersecurity Be a Human Right? Exploring the "Shared Responsibility" of Cyber Peace' (2019) 55 Stanford Journal of International Law 158

——, *The Internet of Things, What Everyone Needs to Know* (Oxford University Press 2020)

Shamir A, 'How to Share a Secret' (1979) 22 Communications of the ACM 612 <https://dl.acm.org/doi/abs/10.1145/359168.359176> accessed 17 May 2022

Shen Y and Vervier PA, 'IoT Security and Privacy Labels' in Maurizio Naldi and others (eds), *Privacy Technologies and Policy, 7th Annual Privacy Forum* (Springer, Cham 2019)

Siddiqui F and others, ‘Secure and Lightweight Communication in Heterogeneous IoT Environments’ (2021) 14 Internet of Things <https://doi.org/10.1016/j.iot.2019.100093>

Siegel J, ‘When the Internet of Things Flounders: Looking into GDPR-Esque Security Standards for IoT Devices in the United States from the Consumers’ Perspective’ (2020) 20 Journal of High Technology Law 189

Sievers T, ‘Proposal for a NIS Directive 2.0: Companies Covered by the Extended Scope of Application and Their Obligations’ (2021) 2 International Cybersecurity Law Review 223

Sion L and others, ‘DPMF: A Modeling Framework for Data Protection by Design’ (2020) 15 International Journal of Conceptual Modeling 1

Sirinam P and others, ‘Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning’, *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (ACM 2018)

Solove DJ, *Understanding Privacy* (Harvard University Press 2010)

Spagnuelo D, Ferreira A and Lenzini G, ‘Accomplishing Transparency within the General Data Protection Regulation’, *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)* (2019) <https://www.datenschutzzentrum.de/uploads/sdm/> accessed 2 December 2021

Spector M and Yadron D, ‘Regulators Investigating Fiat Chrysler Cybersecurity Recall ’ *The Wall Street Journal* (24 July 2015) <https://www.wsj.com/articles/fiat-chrysler-recalls-1-4-million-vehicles-amid-hacking-concerns-1437751526> accessed 14 October 2021

Spindler G and Horváth AZ, ‘SODA Project: D3.5 Use-Case Specific Legal Aspects’ (2019) <https://cordis.europa.eu/project/id/731583/results/it>

Spindler G and Schmechel P, ‘Personal Data and Encryption in the European General Data Protection Regulation’ (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 163

Stahl K and Strausz R, ‘Certification and Market Transparency ’ (2017) 84 Review of Economic Studies 1842

Stallings W and Brown L, *Computer Security: Principles and Practice* (4th edition, Pearson 2018)

Stapko T, *Practical Embedded Security: Building Secure Resource-Constrained Systems* (Newnes 2008)

Sterk LAJ, ‘The Hacker, Product Manufacturer, Sensor Manufacturer, Software Provider or Infrastructure Provider?’ [2018] Thesis LLM Law and Technology Tilburg Law School

<http://arno.uvt.nl/show.cgi?fid=145943>

Stingelin N and others, 'Roles and Functions of Ethics Advisors/Ethics Advisory Boards in EC-Funded Projects' (2012) <https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/ethics-guide-advisors_en.pdf> accessed 12 October 2021

Stockton P and Golabek-Goldman M, 'Curbing the Market for Cyber Weapons' (2013) 32 Yale Law & Policy Review <https://digitalcommons.law.yale.edu/ylpr/vol32/iss1/11> accessed 21 September 2021

——, 'Curbing the Market for Cyber Weapons' (2015) 32 Yale Law & Policy Review <https://digitalcommons.law.yale.edu/ylpr/vol32/iss1/11> accessed 5 October 2021

Sultan A, 'Improving Cybersecurity Awareness in Underserved Populations' [2019] CLTC White Paper Series Berkeley

Sweeney L, 'Simple Demographics Often Identify People Uniquely' (2000) 3

Taddeo M, 'Is Cybersecurity a Public Good?' (2019) 29 Minds and Machines 349

Takbiri N and others, 'Matching Anonymized and Obfuscated Time Series to Users' Profiles' (2019) 65 IEEE Transactions on Information Theory 724

——, 'Matching Anonymized and Obfuscated Time Series to Users' Profiles' (2019) 65 IEEE Transactions on Information Theory 724

Tamò-Larrieux A, *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things* (Springer 2018)

Tanczer L and others, 'IoT and Its Implications for Informed Consent - PETRAS IoT Hub, STEaPP' (2017) <https://discovery.ucl.ac.uk/id/eprint/10050101/1/IoTandConsent_PM_Workshop_Report - 11Comp.pdf> accessed 21 October 2022

Tene O and Polonetsky J, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 Northwestern Journal of Technology and Intellectual Property 239 <https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1> accessed 3 March 2020

The Centre for Information Policy Leadership, 'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR' (2016) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf>

The Danish Institute for Human Rights, 'Human Rights Impact Assessment: Guidance and Toolbox' (2020)

<https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/udgivelser/hria_toolbox_2020/eng/dihr_hria_guidance_and_toolbox_2020_eng.pdf>

The Guardian, 'The Pegasus Project' (*2021*) <https://www.theguardian.com/news/series/pegasus-project> accessed 21 September 2021

Tselios C, Tsolis G and Athanatos M, 'A Comprehensive Technical Survey of Contemporary Cybersecurity Products and Solutions' in Apostolos Fournaris and others (eds), *Computer Security LNCS11981 - ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC* (Springer, Cham 2019)

Tulibacka M, *Product Liability Law in Transition: A Central European Perspective* (Routledge 2016)

Tuominen M and Festor S, 'Initial Appraisal of a European Commission Impact Assessment: Revising the Machinery Directive', vol PE 694.208 (2021) <http://www.europarl.europa.eu/RegData/etudes/note/join/2013/507504/IPOL-JOIN_NT(2013)507504_EN.pdf>

Tzanou M and Karyda S, 'Privacy International and Quadrature Du Net: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28 European Public Law 123

Ullah Z and others, 'Applications of Artificial Intelligence and Machine Learning in Smart Cities' (2020) 154 Computer Communications 313

Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor E, *Handbook on European Data Protection Law* (Publications Office of the European Union 2018)

Urquhart L, Lodge T and Crabtree A, 'Demonstrably Doing Accountability in the Internet of Things' (2019) 27 International Journal of Law and Information Technology 1

van Dam C, *European Tort Law* (Second edi, Oxford University Press 2013)

van de Poel I, 'Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer Science and Business Media BV 2020)

van den Hoven J and others, 'Privacy and Information Technology' in Edward N Zalta (ed), *Stanford Encyclopedia of Philosophy* (Stanford University Press 2020) <https://plato.stanford.edu/entries/it-privacy/#ConVsInfPri>

van der Meulen R, 'What Edge Computing Means For Infrastructure And Operations Leaders' (2018) <https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders> accessed 20 September 2021

Van Der Sloot B, ‘Big Brother Watch and Others v. the United Kingdom & Centrum För Rättvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?’ (2021) 7 European Data Protection Law Review 319

van Diermen R, ‘The Internet of Things: A Privacy Label for IoT Products in a Consumer Market’ (University of Leiden 2018) <https://openaccess.leidenuniv.nl/handle/1887/64571>

Van Erp S, ‘Ownership of Data: The Numerus Clausus of Legal Objects’ (2017) 6 Property Rights Conference Journal 235 <http://www.europeanlawinstitute> accessed 19 April 2022

Van Wel L and Royakkers L, ‘Ethical Issues in Web Data Mining’ (2004) 6 Ethics and Information Technology 129 <https://link.springer.com/article/10.1023/B:ETIN.0000047476.05912.3d> accessed 16 March 2022

Veale M, ‘Knowing without Seeing: Informational Power, Cryptosystems and the Law’ (2019) <https://suri.epfl.ch/slides/2019/michael-veale.pdf>

Veale M and Brown I, ‘Cybersecurity’ (2020) 9 Internet Policy Review 1

Veale M, Nouwens M and Teixeira Santos C, ‘Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?’ (2022) 2022 Technology and Regulation 12

Vecchi D and Turra M, ‘Italy’ in Clinton Davis Varner and Madison Kitchens (eds), *The Product Regulation and Liability Review* (7th edn, Law Business Research Ltd 2020)

Vedder A, ‘Safety, Security and Ethics’ in Anton Vedder and others (eds), *Security and Law* (Intersentia 2019)

Verheul E and others, ‘Polymorphic Encryption and Pseudonymisation for Personalised Healthcare’ (2016) <https://pep.cs.ru.nl/>

Verheul E and Jacobs B, ‘Polymorphic Encryption and Pseudonymisation’ (2017) 5 NAW 168 <http://www.ecc-brainpool.org> accessed 17 May 2022

Voas J, ‘NIST Special Publication 800-183 Networks of “Things”’ (2016) <http://dx.doi.org/10.6028/NIST.SP.800-183> accessed 22 September 2021

Vodafone, ‘A New IoT Regulatory Framework for Europe’ (2019) <https://investors.vodafone.com/sites/vodafone-ir/files/vodafone/our-purpose/social-contract/policy-papers/a-new-iot-regulatory-framework-for-europe.pdf>

Vögler M and others, ‘LEONORE - Large-Scale Provisioning of Resource-Constrained IoT Deployments’ (2015) 30 Proceedings - 9th IEEE International Symposium on Service-Oriented System Engineering, IEEE SOSE 2015 78 <http://www.busybox.net> accessed 31 January 2020

Wachter S, ‘The GDPR and the Internet of Things: A Three-Step Transparency Model’ (2018) 10 Law, Innovation and Technology 266

Wagner G, ‘Software as a Product’ in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Smart Products: Münster Colloquia on EU Law and the Digital Economy VI* (Nomos Verlag 2022)

Waldman AE, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge University Press 2021)

Waldron JJ, ‘Safety and Security’ (2006) 85 Nebraska Law Review 455

Waltz KN, *Theory of International Politics* (Addison-Wesley Publishing Company 1979)

Wan W and others, ‘A Compute-in-Memory Chip Based on Resistive Random-Access Memory’ (2022) 608 Nature 504

Wang J and others, ‘User Behavior Classification in Encrypted Cloud Camera Traffic’, *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings* (Institute of Electrical and Electronics Engineers Inc 2019)

Watkins SG, *An Introduction to Information Security and ISO27001:2013, A Pocket Guide* (Second, IT Governance Publishing 2013)

Wavestone - CEPS - CARSA - ICF, ‘Study on the Need of Cybersecurity Requirements for ICT Products - No. 2020-0715: Final Study Report’ (2021) <https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products>

Weber RH, ‘Internet of Things - Governance Quo Vadis?’ (2013) 29 Computer Law & Security Review 341

Weber RH, ‘Governance of the Internet of Things—From Infancy to First Attempts of Implementation?’ (2016) 5 Laws 28

——, ‘Liability in the Internet of Things’ (2017) 6 Journal of European Consumer and Market Law 207

Weber RH and Studer E, ‘Cybersecurity in the Internet of Things: Legal Aspects’ (2016) 32 Computer Law and Security Review 715

Weber S, ‘Coercion in Cybersecurity: What Public Health Models Reveal’ (2017) 3 Journal of Cybersecurity 173 <https://academic.oup.com/cybersecurity/article/3/3/173/3836936> accessed 5 October 2021

Webster F, *Theories of the Information Society* (Routledge 2014) <https://www.taylorfrancis.com/books/mono/10.4324/9781315867854/theories-information-

society-frank-webster> accessed 4 October 2021

Weiss NE, ‘Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis’ (2015) <https://sgp.fas.org/crs/misc/R43821.pdf> accessed 5 October 2021

Wendehorst C, ‘The Update Obligation – How to Make It Work in the Relationship between Seller, Producer, Digital Content or Service Provider and Consumer’ in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Smart Products: Münster Colloquia on EU Law and the Digital Economy VI* (Nomos Verlag 2022)

Wessel RA, ‘Towards EU Cybersecurity Law: Regulating a New Policy Field’ in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing Ltd 2015)

Wiewiórowski W, ‘Keynote: Data Protection Needs Encryption, EDPS 1st Online IPEN Workshop’ (2020)

——, ‘Keynote: Data Protection Needs Encryption’ *EDPS, 1st Online IPEN Workshop* (3 June 2020)

Wolf M and Serpanos D, *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems* (Springer 2020)

Wolfert S and others, ‘Big Data in Smart Farming – A Review’ (2017) 153 Agricultural Systems 69 <http://dx.doi.org/10.1016/j.agsy.2017.01.023> accessed 19 April 2022

World Economic Forum, ‘The Global Risks Report 2021’ (2021) <https://www.weforum.org/reports/the-global-risks-report-2021> accessed 2 October 2021

Yi S, Li C and Li Q, ‘A Survey of Fog Computing: Concepts, Applications and Issues’ (2015) 2015-June Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) 37

Zanfir-Fortuna G, ‘Personal Data for Joint Controllers and Exam Scripts’ (2018) 2 International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel 12

Zeadally S, Das AK and Sklavos N, ‘Cryptographic Technologies and Protocol Standards for Internet of Things’ (2021) 14 Internet of Things <https://doi.org/10.1016/j.iot.2019.10> accessed 22 April 2022

Zhang H and others, ‘Cloud Storage for Electronic Health Records Based on Secret Sharing with Verifiable Reconstruction Outsourcing’ (2018) 6 IEEE Access 40713

Zhou J and others, ‘Security and Privacy for Cloud-Based IoT: Challenges’ (2017) 55 IEEE Communications Magazine 26

Ziccardi G, *L'odio Online: Violenza Verbale e Ossessioni in Rete* (Raffaello Cortina Editore 2016)

——, 'The GDPR and the LIBE Study on the Use of Hacking Tools by Law Enforcement Agencies' (2018) 4 Italian Law Journal <https://heinonline.org/HOL/Page?handle=hein.journals/italj4&id=223&div=15&collection=journals> accessed 21 September 2021

——, *Tecnologie per Il Potere: Come Usare i Social Network in Politica* (Raffaello Cortina Editore 2019)

Zuiderveen Borgesius F, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) 5 International Data Privacy Law 163

——, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (2017) 3 European Data Protection Law Review 130