The Balance Between Security, Privacy and Data Protection in IoT Data Sharing:

A Critique to Traditional *"Security&Privacy"* Surveys

*Pier Giorgio Chiara**

The paper examines the normative challenges of the Internet of Things (IoT), in particular, taking into account today's debate on privacy, data protection, and security issues brought about by IoT. Three different layers of complexity are under scrutiny. They regard (i) moral and political theories on the concept of 'security'; (ii) whether and to what extent information security technologies, in the context of IoT, may affect fundamental rights, such as privacy and data protection; and, (iii) new legal challenges for individual and group privacy and data protection. The overall aim of the paper is, on the one hand, to stress basic differences between privacy and data protection and why the distinction matters vis-à-vis the flow of information and data sharing on IoT. On the other hand, the intent is to stress the different meanings security has in this context, since the word is often used interchangeably to address information security, cybersecurity, or safety issues. We should take these distinctions firm, when striking balances between privacy, data protection, and 'security' on IoT.

Keywords: Security | privacy | data protection | IoT

I. Introduction

The Internet of Things has been considered by the European Commission as the next step towards digitisation[1]. The rationale of this statement lies in the revolutionary nature of IoT, as it merges physical and virtual worlds. Everyday objects around us, through connected sensors, increasingly collect huge amounts of data which are stored either at device level and processed (e.g. edge computing) or in cloud service platforms. Once stored, data are shared with other devices and parties. The IoT paradigm is of paramount importance for our societies since its application is wide ranging and relate to home appliances, industry, transport systems, health sector, energy sector and, more broadly, smart cities. Against this backdrop, it seems natural that such technology, arguably a game-changer, has attracted, from the very beginning, the attention of lawyers and legislators.

From a methodological standpoint, the research question sets the level of abstraction (LoA) [2] of the legal analysis, integrated with technical aspects. The paper investigates security as well as privacy and data protection issues, among the manifold normative challenges which Internet of Things structural data sharing poses to traditional matters of the law. Having set the context, the LoA can be grasped as a model, or interface, made up by different observables, that is, the features of the legal analysis, which is structured as follows.

DOI: 10.21552/edpl/2021/1/6

* PhD Candidate, Law, Science and Technology, Rights of Internet of Everything; University of Luxembourg | University of Bologna | University of Turin, <https://last-jd-rioe.eu/pier-giorgio-chiara.html>, <piergiorgio.chiara@uni.lu>. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie ITN EJD "Law, Science and Technology Rights of Internet of Everything" grant agreement No 814177.

1 European Commission, "Commission staff working document: advancing the Internet of Things in Europe" (2016) Brussels, 5.

2 Luciano Floridi, "The Method of Levels of Abstraction" (2008) Minds and Machines 18, 303.

The first section of this paper provides for an introduction of the work, highlighting the methodology that has been used.

The second section provides a functional and comprehensive definition, for the purpose of this paper, of the Internet of Things paradigm. The technical investigation will consider a tripartite taxonomy: the model sets three different layers for a better understanding of the structural data sharing i.e., i) device layer; ii) network layer; iii) processing layer.

The third section focuses on the moral and political theories on the concept of 'security'. A preliminary reflection shall delve into the different understandings of security according to traditional moral theories: whether security is an ethical value *per se* or, rather, an instrumental value, say, a necessary precondition for the enjoyment of fundamental goods e.g., fundamental rights. Furthermore, distinguishing between the intertwined concepts of *safety* and *security* might help to appreciate the two conceptions of security at ethical and normative level. We should take the ethical-infraethical distinction of security firm, when discussing Hildebrandt's stance on the allegedly neutral role of encryption vis-à-vis fundamental rights, such as privacy and data protection. Finally, the study investigates whether a clear dividing line can be drawn between the distinct concepts of information and cybersecurity: albeit overlapping, their scope of protection can be distinguished.

The fourth section takes into consideration the new legal challenges for the rights to privacy and data protection brought about by IoT. When it comes to map the privacy debate on the Internet of Things, it is often hard to discern issues related to the right to privacy from data protection ones. Indeed, software engineering literature tends to acknowledge privacy in a holistic fashion, that is to include data protection related concerns without making a due and appropriate distinction, at the normative level. Whereas the e-Privacy Directive currently safeguards the confidentiality of electronic communications, on the other hand, traffic data and location data generated by electronic communications services or devices, as in the case of nearly every IoT system, increasingly "involve personal data processing as well, insofar as they relate to natural persons"[3]. The GDPR, therefore, would always enter into play.

The fifth section concentrates on whether the infraethical role played by cybersecurity might assist when it comes to design risk assessment methodologies for IoT. Given its substantial impact not only on security and privacy, but also on individual safety, IoT significantly amplifies the traditional threat landscape. Risk assessment is indeed a privileged observable under which the interaction between data protection and cybersecurity can be better appreciated, albeit pertaining to different legal domains i.e., private law and criminal law respectively.

Finally, the conclusion sums up the findings regarding the balance between the values at stake in IoT data sharing.

II. Internet of Things Taxonomy: A Technical Overview

The aim of this section is to provide a sufficiently comprehensive overview over data collection and information sharing within the Internet of Things paradigm. From a methodological viewpoint, the *observable* "IoT architecture and design" sets three different variables, say, the interface of the model: device layer; network layer; processing layer. This tripartite taxonomy would reduce the complexity of the IoT architecture, by breaking physical elements and communication processes into smaller and simpler components. The application layer (IoT application domains: industrial, healthcare, transportation etc...) has been intentionally left out from the model since it would exceed the scope of the section, i.e. understanding IoT structural data transmission.

Although the first defining attempts of IoT date back to late 1990s[4], a solid consensus has been recently created around its twofold constitutive nature: an enabling technology for even more complex technologies[5] and a global infrastructure for connecting the physical and the virtual worlds[6]. In other words,

3 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

4 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).

5 ISO/IEC, "Information technology – Internet of Things Reference" (2016) JTC 1/WG 10, Geneva.

6 Stefano Nativi, Alexander Kotsev, Petra Scudo, Katarzyna Pogorzelska, Ioannis Vakalis, Alessandro Dalla Benetta, Andrea Perego, *IoT 2.0 and the Internet of Transformation (Web of Things and Digital Twins)* (2020) European Commission JRC Technical Report, 10.

IoT is a network of things, with clear element identification, embedded with software intelligence, sensors, and ubiquitous connectivity to the Internet[7]. The pervasive and multi-device nature of IoT is increasingly leading to review the original acronym, as some prefers the term Internet of Everything (IoE)[8].

The first layer of the model, i.e. device, considers the "things" in IoT. Sensing, actuating and unique identification are the three key requirements for this level. Sensors are the starting point in IoT data collection: they are electronical 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 [9]. In this respect, three classes of issues arise: emission, as regards the generation of electromagnetic signals; susceptibility, as the tendency to break down under unwanted emissions; coupling, which refers to how the emitted interference reaches some target device[10]. RFID and video tracking are other ways, apart from sensors, to capture and monitor the surrounding environment, i.e. to collect data: 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 or person over a short time interval[11]. Finally, once data is captured and analysed, IoT actuators are in charge of controlling or taking action in IoT systems by converting sensors-collected data to motion[12]. 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[13]: this would affect therefore the other two layers.

Without dwelling too extensively on the complex architecture of IoT network layer, an overview of IoT network models and protocols is nonetheless required. A preliminary consideration should acknowledge that data are sent in IoT networks at all time: "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 system to the homeowner's smartphone while he's in a coffee shop"[14]. As this data are prone to number of attacks (e.g. man in the middle, spoofing, sniffing etc.), it follows that network security is of paramount importance in IoT security. This layer illustrates how IoT components *communicate* within Internet infrastructure. Therefore, it necessarily involves the OSI model and the TCP/IP protocol[15], which provides for end-to-end connectivity detailing the procedure for packetizing, addressing, transmitting, routing and receiving data at the destination[16]. IoT Network layer may 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[17].

The processing layer is a very broad subset of IoT architecture: for the sake of simplicity and clarity, the current processing scenario is plotted in a scalable fashion, according to the needs of mostly IoT resource-constrained devices. Data would firstly be processed "at the edge" (edge computing): in other words, close to the devices who collected them. Then, data will 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 para-

7 Ammar Rayes and Samer Salam, *Internet of Things: from Hype to Reality* (2019), 2nd edition, Springer, 2.

8 CISCO, "How does Cisco define the Internet of Everything, and how is it different from the "Internet of Things"?" (2013), available at: <https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf>; Sandra Khvoynitskaya, "Internet of everything vs internet of things: what is the difference?" (2020), available at: <https://www.itransition.com/blog/internet-of-everything-vs-internet-of-things>.

9 National Research Council, *Expanding the vision on sensors materials* (1995) National academic press, 10.

10 Sonia Ben Dhia, Mohamed Ramdani, and Etienne Sicard (eds.), *Electromagnetic Compatibility of Integrated Circuits: Techniques for low emission and susceptibility* (2006) Springer Science & Business Media.

11 See n 7, 76-80.

12 Id., 82.

13 Carsten Bormann, Mehmet Ersue and Ari Keranen, "Terminology for Constrained-Node Networks" (2014) Internet Engineering Task Force (IETF - 7228), 3.

14 See n 7, 7.

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

16 Mohammed Alani, *Guide to OSI and TCP/IP models* (2014) Springer.

17 See n 7, 48-51.

digm: information processing is located close to the edge, so to speak, where things and people produce or consume that information[18]. 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. Fog computing, albeit conceptually different from edge computing, is indeed similar to edge and cloud technologies[19] as it has been 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 smart end-devices and centralized (cloud) services"[20]. All in all, Fog computing is a computing architecture which uses edge computing devices to carry out a significant part of computation, storage and communication. The rapid data sharing of IoT highlighted the necessity of augmenting the Cloud infrastructure with compute and storage functions that move with the mobile Things: fog computing answers this need by positing its layer of computation between the device and the cloud[21].

III. Disentangling the Security Debate

Security is unquestionably the major challenge for the IoT. Yet, the term "security", taken on its own, comes across as rather abstract and wide ranging, and is therefore difficult to grasp, both in academic literature and in legislative documents.

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 democracy" [22]. The phrasing of the Commission seems to offer a key to interpreting the philosophical debate around security within moral theory, namely whether security has itself an ethical dimension (thus, a fundamental good) or, rather, it is an instrumental value[23]. To contextualize the problem into the present research, 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"[24].

In the words of the Commission, terms such as *basis* and *foundation* suggest that the tension between security, from one side, and safety or fundamental rights (e.g. privacy and data protection), on the other, might not be dealt as a balance within ethics, say, 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)[25]. By infraethics, the philosopher from Oxford means an ethical *infrastructure,* not-yet-ethical so to speak: "the right sort of infraethics is there to support the right sort of axiology"[26] of morally good values, such as fundamental rights (privacy) or personal safety. Put in other words, whereas "ethics governs the axiological evaluation of a state of affairs, infraethics is a set of conditions that facilitate or hider the accomplishment of a morally qualified state of affairs"[27]. All in all, security can also be seen as "an instrumental value to protect moral value"[28], rather than an ethical value on its own: this view is emphasized by the bold statement of Jabri, i.e. "the point at which security is transformed into a universal ethical category

18 Rob van der Meulen, "What Edge Computing Means for Infrastructure and Operations Leaders" (2018), Gartner, available at: <https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/>.

19 Shanhe Yi, Cheng Li, and Qun Li, "A Survey of Fog Computing: Concepts, Applications and Issues" (2015) In Proceedings of the 2015 Workshop on Mobile Big Data, ACM, 37–42.

20 Michaela Iorga et al., "Fog Computing Conceptual Model - Recommendations of the National Institute of Standards and Technology" (2018) NIST Technical report.

21 See n 7, 157.

22 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, Brussels, 24.7.2020 COM(2020) 605, 1.

23 Ugo Pagallo, "Online Security and the Protection of Civil Rights:A Legal Overview" (2013) 26 Philosophy&Technology, 382.

24 Mireille Hildebrandt, "Digital security and human rights: a plea for counter-infringement" (2019) in Mart Susi (ed) *Human Rights, Digital Society and the Law: A Research Companion,* Taylor & Francis, 266.

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

26 Id., 397.

27 Massimo Durante, *Ethics, Law and the Politics of Information: a guide to the philosophy of Luciano Floridi* (2017) Springer, 176-177.

28 Michele Loi and Markus Christen, "Ethical frameworks for cybersecurity" (2020) in Markus Christen, Bert Gordijn and Michele Loi (eds.) *The Ethics of Cybersecurity*, Springer, 76; *contra* see Ibo Van de Poel, "Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security" (2020) in Markus Christen, Bert Gordijn and Michele Loi (eds.) op.cit., 46-71.

is also the point at which it becomes a technology of domination, of the governing over the governed"[29].

Notwithstanding the instrumental value that it can attain, security takes also the form of ethical value[30]. It follows that it can clash with fundamental rights, such as the right to privacy and data protection, which inevitably has to be limited accordingly. Without dwelling too extensively on the distinction between absolute (e.g. prohibition of torture, art. 3 ECHR) and relative (e.g. privacy, art. 8 ECHR) fundamental rights, Pagallo rightly points out that Habermas's distinction between principles and values is fruitful since absolute rights adhere more to the deontological rationale (yes or no) of principles, whilst relative rights, like values, follow the logic of legal balancing[31]. Pursuant to article 52 of the Charter, the limitation of relative rights must be provided for by law and respect the essence of those rights and freedoms; moreover, it has to be subject to the principles of proportionality, necessity and genuinely meet objectives of general interest recognised by the Union. Similarly, limiting the right to privacy, pursuant to article 8(2) ECHR implies a solid legal justification: the infringing measure has to be i) in accordance with the law; ii) necessary in a democratic society; iii) having a legitimate aim. Lawfulness is interpreted as requiring grounds in national law that is adequately accessible, sufficiently foreseeable, so as to anticipate what kind of infringing measures will enforce, and contains effective safeguards, in order to limit such measures either in scope (time and content) or scale[32].

On 6 October 2020, the European Court of Justice confirmed[33] that EU law precludes national legislation requiring a provider of electronic communications services to carry out the general and indiscriminate transmission (Privacy International) or retention (La Quadrature du Net) of traffic data and location data for the purpose of combating crime in general or of safeguarding national security. Nonetheless, the Court ruled that if the Member State is dealing with a serious threat to national security, the ePrivacy Directive[34] and article 23(1) of the General Data Protection Regulation, read in the light of the Charter, do not preclude recourse to an order requiring providers of electronic communications services to retain, generally and indiscriminately, traffic data and location data[35].

Accordingly, security can thus play this double role: it can be argued that the CJEU, consistently with its case-law (cases Tele2 Sverige; Watson and Others; Privacy International and La Quadrature du Net) conceive security within an *infraethical* horizon, in other words as a set of conditions, or an infrastructure, that enable individuals to enjoy fundamental right to privacy, data protection and freedom of expression. Nevertheless, the Court acknowledges situations (whether a Member State is facing a genuine, present or foreseeable threat to national security) where security hinders such rights, playing therefore an *ethical* role.

The inclusion of ethics ensures the alignment of security research and development with principles like fundamental rights, such as data protection and privacy[36], and democracy "instead of quelling these in the name of security"[37]. For the purpose of this study, a functional definition of security is needed in order to sort out the successful facilitations and constraints given by the right infraethics in the context of IoT.

1. The Relation Between Security and Safety

The two strands that security can take (i.e. instrumental or fundamental) might be better appreciated through the distinction between the intertwined concepts of *safety* and *security,* which are often used interchangeably. Durante, engaging with the flourishing and never-ending scholarly debate, acknowledges that whereas "[s]afety is mainly aimed to ensure the

29 Vivienne Jabri, "Security: Critique, analysis and ethics" (2016) in Jonna Nyman and Anthony Burke (eds.) *Ethical Security Studies: A New Research Agenda,* Routledge, 27.

30 Mireille Hildebrandt, "Extraterritorial Jurisdiction to enforce in cyberspace" (2013) 63 Toronto Law Journal 2, 196-224.

31 See n 23, 383.

32 See n 24, 269.

33 The CJEU maintains consistency with its own case-law stemming from the judgment in *Tele2 Sverige* and *Watson and Others*, about the disproportionate nature of general and indiscriminate retention of traffic data and location data.

34 Directive (EU) 2002/58, article 5(1), 15(1), (3).

35 Case C-623/17, *Privacy International*; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, *French Data Network and Others*, and *Ordre des barreaux francophones et germanophone and Others*.

36 European Commission, *Roles and functions of ethics advisors/ethics advisory boards in EC-funded projects* (2012) Brussels, 3.

37 Matthias Leese, Kristoffer Lidén and Blagovesta Nikolova, "Putting critique to work: Ethics in EU security research" (2019) 50 Security Dialogue 1, SAGE Journals, 63.

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"[38]. The philosopher grounds a further level of divergence between the two concepts on a temporal argument: safety has a temporal sphere linked with immediate relationships "(e.g. the violent dimension of time that, according to Locke, does not leave us the time to delegate our decisions to the authority of a third person)", whilst the latter has an intertemporal nature, "mainly part of mediated relationships"[39].

It is non-contentious that IoT implies a paradigm shift, bridging together the physical and cyber environment. Any potential cyberattack on IoT has a direct impact on all the (inter)connected physical objects that are an integrated part of our daily life: such attacks on systems' security may result in physical or psychological damage, affecting the integrity of life: security researchers have shown that an attacker can control remotely implantable and wearable health devices[40] or the brakes of a moving car[41]. Against this background, several authors argue the need to address traditional notions of security and safety more interchangeably, "as security flaws may more often than not be the flip-side of safety risks and vice versa"[42]. It is indeed true that such concepts are deeply intertwined: the EC Communication on "Building Trust in Human-Centric Artificial Intelligence" stated that emerging digital technologies, such as AI systems and IoT, "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"[43]. Scope wise, EU safety legislation aims to ensure that products placed on the Union market meet high health, safety and environmental requirements and that such products can circulate freely throughout the Union[44] (sectorial legislation[45] is complemented by both the General Product Safety Directive and European standards, as further expanded in chapter 3). In the context of IoT security, 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 upon a threat analysis scheme: whereas safety analysis shall start from the *risks* linked to the application domain, security assessments focus prominently on systems' architecture and module design[46]. In other words, despite a holistic understanding, they acknowledge that such concepts operate respectively at different *layers of abstraction*, so to speak, since safety requirements shall include infrastructure security ones: "security is a requirement for safety as well, since data integrity is necessary at least"[47]. Moreover, conceiving security losses as all-or-nothing whilst safety attacks as limited to certain window of time mirrors the abovementioned temporal and intertemporal connotation associated with safety and security.

In conclusion, if the theoretical premise between ethics and infraethics holds on, individual safety and security cannot be used interchangeably even within IoT paradigm. Vedder recognizes indeed the dimensional nature of security, different in its substance from the moral connation of individual safety[48]. Moreover, the *unified* model presented by Serpanos and Wolf is not in conflict either: security requirements have the power to re-shape systems' architecture and design, resulting therefore in a direct influence on safety threats, arising if the constraints or facilitations laid down by security have not been respected.

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

39 Id.

40 Carmen Camara, Pedro Peris-Lopez, and Juan Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey" (2015) Journal of biomedical informatics 55, 272-289.

41 Charlie Miller and Chris Valasek, "Remote exploitation of an unaltered passenger vehicle" (2015) S 91 Black Hat USA.

42 Anton Vedder, "Safety, security and ethics" (2019) in Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (eds.) *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security,* Intersentia, 15.

43 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Building Trust in Human-Centric Artificial Intelligence, Brussels, 8.4.2019 COM(2019) 168 final.

44 Report from the Commission to the European Parliament, the Council and the European Social Committee on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, Brussels, 19.2.2020 COM(2020) 64 final, 3.

45 Such as transport and cars legislation.

46 Dimitrios Serpanos and Marilyn Wolf, *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems* (2020) Springer Nature, 35-36.

47 Dimitrios Serpanos and Marilyn Wolf, *Internet-of-Things (IoT) Systems – Architectures, Algorithms, Methodologies* (2018) Springer Nature, 55-76.

48 See n 42, 14-15.

2. Security as an Ethical Value: The Allegedly Neutral Nature of Information Security Technologies vis-à-vis Fundamental Rights

When it comes to address security as an ethical value, as it has been already stressed, a balance with fundamental rights is likely to occur". Following the tripartition of information security technologies made by Hildebrandt, the key takeaway is that digital security technologies generate paradoxically new digital security risks and violation of fundamental rights as the State, through law enforcement or intelligence, claims the supremacy of security over liberties[49]. Hildebrandt argues that the trusted parties on which encryption relies on can violate their duties; authentication technologies allow for monitoring; monitoring is in turn linked with surveillance, threatening therefore the right to privacy and non-discrimination legislation; filtering and blocking can be deemed a violation of net neutrality principle[50]. Against this backdrop, the "governance of encryption" debate can be taken as a case-study: whereas encryption is widely recognised by EU data protection actors as a prominent security measure[51], law enforcement and intelligence services advocate for the creation of means (i.e., backdoors) allowing to circumvent security solutions that cryptography provides to contrast heinous digital crimes and for national security purposes (i.e. public goods). Recently, the governments of UK, US, Australia, New Zeland, Canada, Japan and India jointly published a public statement on (end-to-end) encryption which openly assert that public safety cannot be protected without compromising privacy or cyber security[52], whereas Apple is increasingly committed to empower users in dealing with an app's privacy practices[53].

In order to resolve this quandary, it seems necessary to resort to the preliminary distinction between infraethics and ethics. Thus, the EU seems to have chosen a different path. As stressed above, it is non contentious that the scope of fundamental rights could be limited, either when faced with public goods, e.g. national security, which in turn they may provide for the enjoyment of fundamental rights themselves or because different rights need to be aligned. Notwithstanding, by setting the right sort of infraethics, i.e. the instrumental values we want to assign to security, the axiological state of affairs will be determined accordingly, avoiding thus trade-offs.

Firstly, to put a halt on this debate, European Parliament, when discussing ePrivacy Regulation amendments, proposed a set of constraints (towards Member States attempts of breaking encryption) and facilitations (towards privacy and security of individuals' electronic communications), say, an infraethics, in order "to safeguard security and integrity of networks and services [and] to forbid Member States from imposing any obligation on encryption providers, on providers of electronic communications services or on 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"[54].

Secondly, the Council of the European Union released a new draft resolution on end-to-end encryption: the position of the Council is clear. And radically opposed to the recent statement of UK&US. Thus, *security* is not balanced with fundamental rights, i.e. privacy, data protection and freedom of expression, involving therefore trade-offs: "[p]rotecting the privacy and security of communications through encryption and at the same time upholding the possibility for competent authorities in the area of security and criminal justice to lawfully access relevant data for legitimate, clearly defined purposes in fighting serious and/or organized crimes and terrorism, including in the digital world, are extremely important"[55].

Without dwelling to extensively on the case law of the CJEU, it can be argued that the Court conceive security within an *infraethical* horizon, by setting conditions that enable individuals to enjoy fundamental

49 See n 24, 262-265.

50 Id., 264.

51 High Level Group of Scientific Advisors, "Cybersecurity in the European Digital Single Market" (2017) SAM, Scientific Opinion No. 2/2017, 31; ENISA, "ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards our Digital Identity" (2016), 5.

52 UK Government, "International statement: end-to-end encryption and public safety" (2020), available at: <https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety/international-statement-end-to-end-encryption-and-public-safety-accessible-version>

53 Apple, see: <https://developer.apple.com/news/?id=hx9s63c5>

54 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).

55 Council of the European Union, "Draft Council Resolution on Encryption - Security through encryption and security despite encryption" (2020), 3.

rights: a *general and indiscriminate* power of breaking encryption would fall to meet either article 52 of the Charter or the triple test for limiting the right to privacy, say. Against this backdrop, the principles of proportionality, necessity and lawfulness shall assess whether the threshold for a justifiable balance is met. This leads to Hildebrandt's claim for a "freedom infringement impact assessment" for digital security technologies, resulting in evidence-based measures[56].

All in all, it is a design issue: the European values and principles, highlighted in the document, would be inconsistent with the easy path leading to a *backdoor by default* society, surreptitiously invoked by other international actors. Believing that it is not a zero-sum game, the Council aims at designing a framework where potential technical solutions are subject to proportionality, necessity and judicial oversight (cfr. art. 52(1) Charter), while upholding fundamental rights and preserving the advantages of encryption[57].

3. Shades of Security in the Cyberspace

A definition of security that could fit the IoT landscape shall necessarily start from the conceptualisation of the broad notion of cybersecurity. Back to 2013, the European Commission established "cybersecurity" as a new community policy area with the release of the First EU Cybersecurity Strategy[58]. The first legislative initiatives in this field saw a divergent approach between US and EU: the former generally conceived cybersecurity as the ability to protect or defend the use of cyberspace form cyberattacks[59], whereas the latter initially flattened the concept on network and information security related aspects, i.e. the integrity and availability of the networks and the confidentiality of information transmitted *via* such infrastructure. Before the term cybersecurity gained hype, though, reflections on how to secure the cyberspace revolved around the concept of "computer security" which, in turn, could be ideally divided into "information security" and "system security"[60], now subsets of cybersecurity[61]. Traditionally, the concept of information security underpins the understanding of security oriented towards the protection of data and information[62], whilst the latter aims at ensuring that systems operate as designed.

Against this background, NIS Directive (Directive EU 2016/1148) was meant to provide a regulatory framework for cybersecurity. The notion of cybersecurity has been recently reshaped by European legislator with Regulation EU 2019/881 (henceforth, Cybersecurity Act) as the set of activities necessary to protect the network and information systems, the users of these systems and any other people involved in cyber threats[63]: the Commission intentionally left as broadly such understanding so to encompass a broad range of governance risks without conceptualising it in an unduly limited fashion[64]. Given the view of (national) security as a critical sphere where everyone is involved, the level of safety of both individuals and businesses in cyberspace is itself a relevant value. Finally, on 16 December 2020, the Commission presented a new EU Cybersecurity Strategy, laying down the framework within which the Proposal for a NIS 2.0 and the Proposal for a Directive on the Resilience of Critical Operators of Essential Services are implemented. Consistently with previous strategies, Bruxelles acknowledges that improving cybersecurity is essential, on the one hand, to trust and benefit from innovation, connectivity and automation; on the other hand, for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information.

Yet, another connotation of security as an instrumental value can also be found in the GDPR, after a careful reading of article 1(2). The Regulation aims to protect the fundamental rights and freedoms of individuals, and security, enucleated foremost in arti-

56 See n 24, 270.

57 See n 55, 4-5.

58 European Commission and High Representative, "Cybersecurity strategy of the European Union: an open, safe and secure cyberspace" (2013), 3.

59 NIST, "Cybersecurity" Glossary, available at: <https://csrc.nist.gov/glossary/term/Cyber_Security>; see also Ronald Ross, "Managing Information Security Risk: Organization, Mission, and Information System View" (2011) NIST Special Publication 800-39, 63.

60 Dominik Herrmann and Henning Pridöhl, "Basics concepts and models of cybersecurity" (2020) in Markus Christen, Bert Gordijn and Michele Loi (eds.) *The Ethics of Cybersecurity*, Springer, 11.

61 ENISA, "ENISA overview of cybersecurity and related terminology" (2017), 6.

62 Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri, "An Introduction to Information Security" (2017) NIST Special Publication 800-12.

63 Regulation (EU) 2019/881, article 2(1)(1).

64 Gloria González Fuster and Lina Jasmontaite, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights" (2020) in Markus Christen, Bert Gordijn and Michele Loi (eds.) op.cit. 103.

cle 32, is one of the core principles around which the intent of protection is based: *security as infraethics* implements therefore an infrastructure for the enjoyment of fundamental primary goods, i.e. rights and freedoms. The EU security strategy acknowledges that cooperation between ENISA, data protection authorities and the European Data Protection Board is of utmost importance in fulfilling the most important long-term need, i.e. developing a culture of cybersecurity by design[65]: "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"[66]. The CJEU has consistently enlightened, since the Case *Commission v Austria*[67], that ensuring the requirements of information security is "an essential component of the protection of individuals with regard to the processing of personal data"[68].

Beyond the all-encompassing notion of cybersecurity, the question is whether within the narrower field of information security is possible to facilitate or protect integrity of individuals (the moral value of individual safety) and the enjoyment of the fundamental rights to privacy and to data protection. To answer this question, however, it is necessary to cast the light on the challenges posed to individuals' rights by IoT architecture and data sharing design.

IV. The Alignment of Privacy and Data Protection in IoT Data Transmission

When it comes to map the privacy debate on the Internet of Things, it is often hard to discern issues related to the right to privacy from data protection ones. Indeed, software engineering literature, or more generically the so-called "technical community" as opposed to legal researchers, tends to acknowledge privacy in a holistic fashion, that is to include data protection related concerns without making a due and appropriate division. Konoudes and Kapitsaki, carried out a systematic literature review to identify the state of the art of user privacy protection in IoT: out of 84 papers reviewed, 58 contain the word "privacy" in the title, whilst only 6 do include "personal data" or "data protection"[69]. Nonetheless, all the examined works are classified pursuant to several challenges of applying GDPR requirements that have been previously identified. The danger of this trend, which has its roots in the US reconstruction of privacy frameworks and values[70], is that the incorrect framing of the problem will be reflected in a bad legacy at legal level.

The right to privacy is indeed closely related to the right to data protection. Kokott and Sobotta's goundbreaking article clearly sets out the boundaries of the problem. On the one hand both aims to protect similar fundamental values, i.e. the *autonomy* and *human dignity* of people [emphasis added], by granting them a personal sphere in which they can freely develop their personality, shape their opinions and ideas[71]. Indeed, the European approach emphasizes the understanding of dignity, which combines intimacy with respect, contributing to define the position of each person in society: the former "has the flavour of something inviolable and inalienable, whilst the latter has to do with everyone´s relationships with everyone else"[72]. On the other hand, albeit substantial overlaps, these rights have different scopes and rationales[73]. The Charter of Fundamental Rights of the European Union (hereafter, 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), also covered by

65 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, Brussels, 24.7.2020 COM(2020) 605.

66 Communication on 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) 264, 10.

67 Case C-614/10, *Commission v Austria,* 2012.

68 Nora Ni Loideain, "A port in the data-sharing storm: the GDPR and the Internet of things" (2019) Journal of Cyber Policy, 11.

69 Alexia Kounoudes and Georgia Kapitsaki, "A mapping of IoT user-centric privacy preserving approaches to the GDPR" (2020) 11 Internet of Things, 1-18.

70 The Stanford Encyclopedia of Philosophy even goes so far as to say that the European approach "conceptualizes issues of informational privacy in terms of data protection", whilst US scholars in terms of privacy (Stanford Encyclopedia of Philosophy, 2019).

71 European Union Agency for Fundamental Rights, *Manuale sul diritto europeo in materia di protezione dei dati* (2018) EU publishing office, Luxembourg, 20-21.

72 Stefano Rodotà, "Privacy, libertà e dignità: Discorso conclusivo della Conferenza internazionale sulla protezione dei dati" (2004) 26th International Conference on Privacy and Personal Data Protection.

73 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 4; Deni Elliott, "Data protection is more than privacy" (2019) 5 European Data Protection Law Review 1, 13–16; 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 3, 569–597.

article 8 of the European Convention on Human Rights (ECHR), and the right to the protection of personal data (art. 8)[74]. Several authors, such as Pagallo, Gutwirth and De Hert, conceived the relation between the twos in terms of, so to speak, protection of individuals' "opaqueness" *versus* "transparency" of the collection and processing of personal data[75]: whereas privacy refers to the holistic intertemporal protection of individuals' inner dimensions, (personal) data protection rights, triggered when people start allowing information to get out of that private sphere, aim at demanding the transparency of such processing. Albeit the above-mentioned and non-contended distinction, as noted by Fuster and Hijmans, "the two rights are clearly coupled in the relevant case law of the CJEU, where they are not *systematically* distinguished – and where they are occasionally presented in complex interwoven manners"[76].

In the context of IoT computing, data transmission may cast the light on the so-called realignment of privacy and data protection: communication, here, is conceived as any data transfer occurring at any layer constituting IoT ecosystem[77].

1. How the Pervasiveness of "Personal Data" in IoT Communication Triggers both ePrivacy Law and the GDPR

The aim of this section is to cast the light on the blurred and over-comprehensive notion of *personal data,* leading to the application of the GDPR, when it comes to address IoT communication content data and possibly metadata. The intention, here, is neither to draw a traditional typology of privacy theories[78] or a taxonomy on privacy harms[79], nor to suggest that the GDPR covers only the right to data protection[80], whereas the right to privacy in electronic communications is exclusively safeguarded by the ePrivacy Directive or upcoming Regulation: rather, whether and to what extent the material scope of these European instruments is triggered by IoT structural data sharing. Thus, one of the legal challenges brought on by the structural data sharing and multilayered architecture of IoT is the realignment of privacy and data protection[81].

Whereas EU data protection law, i.e. the GDPR, is not all about confidentiality, e-Privacy Directive currently safeguards the confidentiality of electronic communications[82], awaiting the incoming e-Privacy Regulation[83]: the recent turnover in the presidency of the EU Council has led to a discussion paper on the proposed e-Privacy Regulation on 6 July 2020, based on Croatian Presidency's latest compromise proposal from 6 March 2020[84]. Importantly, the new Recital 12 would explicitly ensure full protection of the rights to privacy and confidentiality of communications to machine-to-machine and Internet of Things services, unless IoT transmission is carried out via a private or closed network such as a closed factory network[85].

The highly intensive regime of EU data protection law, say, the GDPR, is likely to enter into play in near-

74 Opinion of AG Sharpston, 27 September 2018, Case C 345/17, *Buivids,* § 61.

75 Serge Gutwirth and Paul De Hert, "Regulating Profiling in a Democratic Constitutional State" (2008) in Mirelle Hildebrandt and Serge Gutwirth (eds) Profiling the European Citizen, Springer, 271; Ugo Pagallo, "The Group, the Private, and the Individual: A New Level of Data Protection?" (2017) in Linnet Taylor, Luciano Floridi and Bart Van der Sloot (eds.) Group Privacy, Springer International Publishing, 159.

76 Gloria González Fuster and Hielke Hijmans, "The EU rights to privacy and personal data protection: 20 years in 10 questions" (2019) International Workshop Exploring the Privacy and Data Protection connection, 4; see also Case C-73/16, 27 September 2017, *Puskar*, §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".

77 A holistic view on data transmitted through electronic communication networks, as to include both content and metadata, is strongly endorsed by EDPS (EDPS, Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications) and Article 29 Working Party (Article 29, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation, WP 247).

78 Bert-Jaap Koops et al., "A typology of privacy" (2017) 38 University of Pennsylvania Journal of International Law 2, 483-575.

79 Daniel Solove, *Understanding privacy* (2008) Harvard University Press, GWU Legal Studies Research Paper No. 420.

80 Article 1(2) of the GDPR can be conceived as to include the right to privacy in the scope of the Regulation.

81 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" (2017) in Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul de Hert (eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures*, Springer, 59.

82 ePrivacy Directive, article 3: the Directive applies to "publicly available electronic communication services and electronic communication network".

83 See Recital 12 of the Proposal for so-called ePrivacy Regulation.

84 Emma Finlayson, "German Presidency of the Council of the EU takes on the draft ePrivacy Regulation" (27 July 2020) Osborne Clarke.

85 German Presidency Draft document on ePrivacy Regulation, September 2020, available at: <http://downloads2.dodsmonitoring.com/downloads/EU_Monitoring/2020-09-24_Projet_e-privacy_Allemagne.pdf>.

ly every IoT scenario: albeit the European Commission acknowledged the value of non-personal data usage in industrial/manufacturing data space[86], privacy and (personal) data protection concerns arise even in the context of Industrial Internet of Things (IIoT)[87], an application domain that should arguably be dominated by non-personal data. All in all, not only the definition of "personal data" is intentionally designed as broadly by the European legislator[88], but also the identifiability criterion is dynamic and context-dependent, which, similar to "relate to" [89], cannot be established in an absolute way[90]. It results that legal certainty is even more difficult to obtain.

To make things more complex, the GDPR standards and principles will apply not only to electronic communication content data, but also to metadata. The Regulation does not *explicitly* address metadata in the context of electronic communications. Thus, article 95 and recital 173 GDPR set out the indisputable *lex generalis-lex specialis* relationship between GDPR and ePrivacy Directive: as long as more specific safeguards are laid down in the e-Privacy Directive, GDPR's general framework will not apply.

Things will not change with the ePrivacy Regulation. Dumortier et al. valuably noted that "[t]he lack of inclusion of any metadata within article 9 of the GDPR can be seen as a recognition that this type of information is not sensitive per se – as is the case with the types of data in Articles 9 and 10 – but that its sensitivity depends on the context and thus needs to be assessed on a case-by-case scenario for each individual processing"[91].

On the one hand, traffic data, i.e. metadata, generated by electronic communications IoT services or devices, increasingly "involve personal data processing as well, insofar as they relate to natural persons"[92]. On the other hand, recent researches have valuably demonstrated that traffic data such as timestamps related to encrypted data packets[93], can arguably be deemed personal data, even though, *prima facie,* they fall outside any definition of personal data: illegal profiling from adversarial inferences of network timing patterns in IoT devices shows that serious privacy and data protection concerns may arise even if security techniques such as encryption are adopted[94].

Albeit the sensitive nature of metadata is widely acknowledged[95], Article 29 Working Party, commenting on the proposal for ePrivacy Regulation, singles out as a point of "grave concern" the different level of protection accorded to content and metadata[96]. Dumortier et al. conclude that the ePrivacy Regulation would fall short to consider that *every* processing of metadata may be sensitive. Therefore, a data protection impact assessment shall be required, following the risk-based approach of the GDPR. Notwithstanding, under current article 6.2 of the Proposal, if the processing is necessary to ensure the operation of electronic communications services, the processing is automatically considered lawful and data protection impact assessment would not be required. "A re-orientation of the approach of the e-Privacy Regulation that [e]nsures an equal approach for functionally identical services with identical data protection risks, seems preferable"[97].

86 European Commission "A European Strategy for Data" (2020), 22.

87 Chunjong Yin et al., "Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things" (2018) 14 IEEE Transactions on Industrial Informatics 8, 3628-3636; Ashok Kumar Das et al., "Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment" (2018) 5 IEEE Internet of Things Journal 6, 4900-4913; Ahmad-Reza Sadeghi et al., "Security and privacy challenges in industrial Internet of Things" (2015) 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 1-6.

88 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).

89 Regulation (EU) 2016/679, article 4(1).

90 Regulation (EU) 2016/679, Recital 26.

91 Jos Dumortier et al., "Legal memo with respect to the concept of metadata and its degree of sensitivity under future European e-privacy law" (2018) Time Lex position paper, 10.

92 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

93 Jingjing Ren et al., "Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach" (2019) Proceedings of the Internet Measurement Conference, 267-279; Abbas Acar et al., "Peek-a-boo: i see your smart home activities, even encrypted!" (2020) Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 207-218; Nazanin Takbiri et al. "Matching anonymized and obfuscated time series to users' profiles" (2018) 65 IEEE Transactions on Information Theory 2, 724-741.

94 Pier Giorgio Chiara, "The Unsecure Side of (Meta)Data in IoT Systems" (2020) 28 Intelligent Environments, IOS Press, 112.

95 Joined Cases C-203/15 and C-698/15, *Tele2 Sverige,* §99.

96 Article 29 Data Protection Working Party, "Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)" (2017).

97 See n 92, 18.

As shown in section III(2), the *observable* encryption shall cast the light on the alignment of privacy, data protection and information security beneath IoT communications. Encryption is undoubtedly "the" means of ensuring confidentiality of communications, as it guarantees the right to privacy of individuals in the cyberspace. At the same time, it provides for cybersecurity, here conceived in terms of information security. The GDPR, envisages encryption as means to assure the principles underpinning information security: the European Data Protection Supervisor claimed it as "natural mean for data protection, and for personal data protection as well: GDPR, in this sense, is reflecting a natural state"[98].

V. The Infraethical Value of Cybersecurity in IoT Risk Assessment

In an increasingly digitalised and information-driven society, the security debate easily spills over onto the cyber and information security domains: the question ultimately boils down to whether the infraethical perspective might also be applied to the interface between cybersecurity and the fundamental rights to data protection and privacy. This section aims to shed the light on the infraethical role played by cybersecurity in the IoT field, especially as regards risk assessment, an area of interaction between data protection and cybersecurity. The resulting evolving and highly fragmented field of cybersecurity risk management is a horizontal problem, "which is in a sense a common denominator of various new technologies connected to the World Wide Web"[99], including therefore IoT. ENISA already pointed out that, as there is no common EU-wide approach to cybersecurity in IoT, or a common multi-stakeholder model on cybersecurity, most companies and manufacturers are taking their own approach when implementing security into IoT, resulting in a lack or slow embracement of standards to guide the adoption of IoT security measures and good practices[100].

On the one hand, IoT is already re-shaping the concept of risk, as it was traditionally understood. As shown in section III(1), the traditional IT security threat landscape is enriched by risks to individuals' safety, as the connected objects interact with and within the physical dimension. On the other hand, risk assessment represents a key pillar of the GDPR risk-based approach[101]. The GDPR displays a strict link between security and risk management as it adopts a risk-based approach not only in laying down data security requirements, but mandating "a risk management strategy, as demonstrated by the controller's obligations concerning the records of the processing activities (art 30), data protection impact assessment (DPIA), prior consultation (arts 35 and 36) and data breaches (arts 33 and 34)"[102]. Whereas existing DPIAs schema embed technical security measures as part of the assessment, traditional risk analysis models in the field of information security see privacy and data protection requirements as subset of the overall process[103]. The hiatus boils down to the rationale of the assessments: the former aims at safeguarding individuals' *fundamental rights and freedoms*[104]; the latter aims at protecting *the assets of the organisation*[105]. Holistic risk analysis methodologies, aiming at combining the two aspects, are needed to encompass the breadth of security considerations to tackle, eschewing therefore the horizon of an insecure society: securing the whole IoT architecture and supply chain[106] would be prodromal to safeguard individuals from personal data processing risks.

Against this background, the infraethical role of cybersecurity can be appreciated when it comes to choose the appropriate security measures to prevent

98 Wojciech Wiewiórowski, *Keynote: Data protection needs encryption,* EDPS, 1st Online IPEN Workshop, 3 June 2020.

99 See n 64, 98.

100 ENISA, *Baseline Security Recommendations for IoT in the context of critical information structures* (2017), 53.

101 Alessandro Mantelero, "Comments to Articles 35 and 36" (2020) in Mark Cole and Franziska Boehm (eds.) *GDPR Commentary*, Edward Elgar Publishing, forthcoming; see also 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 1.

102 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, 4.

103 ISO/IEC technical standard 27701:2019 is an extension to ISO/IEC 27001:2013: it provides for support compliance with the GDPR by promoting a hierarchy that subordinates data protection to information security.

104 GDPR article 35; Article 29 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" (2017) WP 248, 6.

105 Raffaella Brighi, "Vulnerabilità e sicurezza: un'analisi informatico-giuridica di concetti in evoluzione" (2019) XXXV Notizie di Politeia 136, 38.

106 ENISA, *Guidelines for securing the Internet of things – secure supply chain for IoT,* (2020).

and mitigate the risk. In other words, a good infraethical construction of cybersecurity measures that is oriented towards facilitating the occurrence of what is morally good, that is, the protection of personal data and the safeguard of rights and freedoms of individuals. This theoretical reconstruction finds an institutional brick wall in the EU Commission cybersecurity strategy of December 2020: "[i]mproving cybersecurity is therefore essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information"[107]. Hence, cybersecurity is essential for upholding fundamental rights and liberties. The infraethical perspective still holds on.

VI. Conclusions

Security, privacy and data protection are the most visible challenges in IoT. The novel contribution to the scholarship in this paper is the analysis of the different values these concepts may attain within IoT paradigm. Thus, when striking balances between security and fundamental rights, such as privacy and data protection, the right level of abstraction has to be set accordingly: security can attain an *infraethical* understanding, that is a precondition for the legal framework on which *ethical* fundamental rights rely; on the other hand, it is at times conceived as ethical value, involving therefore trade-offs or balances with human rights.

First of all, when it comes to map the IoT security debate, the intertwined yet distinct rationales of security and safety shall be firm, as security threats, risks and vulnerabilities can affect individuals' safety: future models of IoT governance shall centre on overarching mechanisms to ensure proper safety and security management.

Moreover, IoT structural data sharing will increasingly highlight the critical role of information security technologies, such as encryption, under which an alignment of the rationales of cybersecurity, information security, privacy and data protection can be appreciated. The tension between cyber and information security, on one side, and the fundamental rights to data protection and privacy, on the other, might not be dealt as a balance within ethics, say, moral rights on the same level but, rather, in infraethical terms.

Against this background, IoT risk assessment has been chosen as a key interface between data protection and cybersecurity. Future models of governance need to consider *risk* from a holistic standpoint. By leveraging the infraethical role of cybersecurity, the *appropriateness* of the technical and organizational security measures that are to be implemented can be better appreciated. That is, a good design of cybersecurity measures, aimed at upholding the protection of fundamental rights, such as privacy and data protection, and freedoms of individuals. If cybersecurity is implemented responsibly, the IoT can foster innovations that enhance functionality; implemented poorly, it eases the emergence of risks to physical safety, data protection and privacy that are not holistically envisaged by current regulatory frameworks[108].

---

107 European Commission, "The EU's Cybersecurity Strategy for the Digital Decade" (2020), 4.

108 Irina Brass and Jesse H. Sowell, "Adaptive governance for the Internet of Things: Coping with emerging security risks" (2020) Regulation & Governance, 16.