Complexity of IoT technologies: European regulations in progress and patterns of customer communication*

Chiara Vescovi

Abstract

Internet of Things devices generate ecosystems that enter the households of customers and influence their everyday life. Therefore, in building these technologies, manufacturers are called upon to assess the cultural and digital context and the effect of digitalisation in end-users, who expect products to be trustworthy, safe, and compliant with the needs brought up by a fast-changing digital world. The European Union is adopting a multidisciplinary approach in the attempt to regulate a highly horizontal matter, impacting people and markets. The article analyses the last legislative proposals, balancing the right of consumers and the efforts required to manufacturers to comply with a responsible approach to these technologies. Building a trusting communication channel between stakeholders may be the only feasible approach, as legislative solutions can help but rarely will be (alone) able to solve all issues related to such a pervasive technology.

I dispositivi connessi generano ecosistemi di prodotti e funzionalità che entrano nella quotidianità e nelle dimore dei consumatori. Pertanto, i produttori vengono chiamati a rispondere non solo della conformità dei prodotti, ma anche a considerare il contesto culturale e digitale nel quale essi sono inseriti e gli effetti della digitalizzazione sui consumatori finali, che si abituano a confrontarsi con un mondo che cambia di pari passo con la tecnologia. Nel tentativo di regolare al meglio un fenomeno che impatta cittadini e mercati, l'Unione Europea adotta un approccio multidisciplinare, che l'articolo si propone di ripercorrere. L'analisi si concentra sugli investimenti richiesti ai produttori di tecnologia IoT per realizzare dispositivi che rispettino i criteri di responsabilità e i diritti dei consumatori. La soluzione proposta è la costituzione di un canale comunicativo e di fiducia tra produttori e consumatori, che sia complementare a soluzioni legislative non sempre soddisfacenti in caso di tecnologie così innovative e pervasive.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Summary

Keywords

Internet of Things - Artificial Intelligence - Data Act - European Union - consumer protection

1. Regulating the Internet of Things: A European perspective

When computing and smart devices are synchronized with physical hardware the output generated is known as Internet of Things[1] (or IoT) as the «connection between the physical and the cyber systems allows a seamless transfer of data (through network connectivity) without any interference from users».[2]

Mankind has always had the tendency to substitute manpower with machines when a person providing a task resulted less efficient and slower than a machine.[3] This attitude is a direct consequence of a technical and technological revolution which had been going on for years and, understandably, experienced an acceleration in the past years with the advancement of studies in Machine Learning and Artificial Intelligence, making data analytics more common, easier, and referred to a larger quantity of data.[4]

The attractiveness of the IoT technology goes back to 1970s when it was known as "embedded internet". [5] Pushed by large commercial giants such as Procter and Gamble, Google, and Gartner[6] it had various instant of glories up until today, when learning technologies entered our everyday life and our households through supports such as smart home assistants and the wearable devices. IoT applications are invading many different areas of our everyday life: affecting education[7], driving, cooking, sport

[1] F. Gregorio et al., *Internet of things in Signal Processing Techniques for Power Efficient Wireless Communication Systems*, New York City, 217 ss.

[2] A. Saeed et al., *Energy Efficient Hybrid IoT System for Ambient Living,* Switzerland, 2022.

[3] N. Wiener, *The Human use of Human Beings – Cybernetics and Society*, Cambridge, 1950.

[4] R. Khan, *Future internet: the internet of things architecture, possible applications and key challenges*, 257 ss.

[5] A. Saeed, *A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems*, 18.

[6] A. Saeed, *A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems*, cit.

[7] I. N. Mseer, *Internet of Things and Its Impact on the Future of Education*, Switzerland, 2021.

and living; but became also a valuable support to improve system reliability, security and safety thanks to predictive maintenance, statistical analysis, and estimations.[8]
Advanced technologies introduced models and standardisation[9] into our reality: reproducing and ameliorating human patterns that have been studied and analysed deeply. Standards provide use cases for rules, harmonize requirements and «even more than general standards, ICT standards have a vital economic interest as they foster progress in creating more efficient and interoperable components of new technological objects. However, they can also constitute a barrier to the market»[10] therefore legislators shall be aware of the burden that standards bring with them.

1.1. The beginning

The European Commission interest in IoT and its legislative perspective goes way back and already in 2009, it addressed Internet of Things as "an umbrella for a new paradigm."[11] An emerging interest for the protection of personal data and awareness in dealing with technical innovations (which were, indeed, about to become some of the main concerns of the European Union) contributed to the popularity of the IoT conversations. Reasonings and studies on the best way to deal with new technologies kept flowing and scholars started to deliver some requirements that would have had to be kept in mind in regulating the Internet of Things.[12]
Among others, in 2010 Professor Rolf H. Weber listed four characteristics of IoT[13] that must be considered when dealing with this type of technology: understanding them is intrinsically linked to a correct governance of their inputs and outcomes.

- *Globality*, i.e., the trans-border element, embedded in products and services connected with networks.
- *Verticality*, meaning the durability of the products, which if connected can usually be updated and therefore extend their lifespan through upgrades and more efficient algorithms.
- *Ubiquity*, referring to the fact that the same product or service can be accessed simultaneously by different persons and from different places.
- *Technicity,* which stands for the necessity to consider the technical complexity of the devices connected.

New rules and legislations that are spawning within the EU institutions shall consider

[8] B.C. Kavitha - R. Vallikannu, *Fault Detection and Data Management for IoT*, in *Multimedia Technologies in the Internet of Things Environment*, 93, Singapore, 147 ss.

[9] F. Gennari*, Standard Setting in Organitsations for the IoT: How to Ensure a Better Degree of Liability?,* in *Masaryk University Journal of Law and Technology*, 15, 2021, 153 ss.

[10] Ivi, 155.

[11] Commission of the European Communities, *Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions*, Internet of Things — An action plan for Europe.

[12] R. H. Weber, *Internet of Things – New security and privacy challenges*, in *Computer Law & Security Review*, 26, 2010, 23 ss.

[13] R. H. Weber, *Internet of Things – New security and privacy challenges*, cit., 23-30.

the previous as a common ground on which building provisions that are adaptable with innovations connected with this technology.

1.2. The European answer to a business opportunity

Besides being instruments of efficiency and development, nowadays IoT devices represent an almost irreplaceable asset for companies, as they «will [keep] foster[ing] an exponential growth in the volume, quality, and variety of consumer-generated data».[14] Moreover, the "monetary value" of consumer data[15] increases the larger the number of data processed, as «informational goods are non-rival in nature. Hence, economic welfare will typically increase by data sharing».[16]

The vastity of the market surrounding IoT devices was confirmed in 2022 by the European Commission that in its final report on consumer Internet of Things affirmed that:

«As the use of consumer IoT products is increasingly becoming part of everyday life for Europeans, the consumer IoT sector is expected to grow significantly in the coming years. It is predicted that overall consumer IoT revenue worldwide will grow from EUR 105.7 billion in 2019 to approximately EUR 404.6 billion by 2030. European smart home revenue will also more than double between 2020 and 2025 (from approximately EUR 17 billion to approximately EUR 38.1 billion)[17]».

Such economic value shall be supported by a solid legislative framework, able to enhance the business development while protecting the rights of citizens and consumers. Therefore, it is no coincidence that, looking at the legal initiatives the European Union is working on, some documents seem to be destined to have a calculated interest in the IoT market.

In the present paper some of the initiatives proposed by the Union will be analysed more in depth, to better understand their value for IoT technologies. They are:

- The proposal for a Data Act[18], a programmatic document which aims at governing data generated by IoT devices, with a strategic approach.
- Two cybersecurity initiatives:
    - the Cybersecurity Act[19], in force since 2019, which established a European cybersecurity certification scheme managed by the European Union Agen-

[14] S. Elvy, *A commercial law of privacy and security for the internet of things*, Cambridge, 2021, 244.

[15] P. M. Schwartz, *Property, Privacy and Personal Data*, in *Harvard Law Review*, 117, 2004, 2055 ss.

[16] J. Drexl, *Access as a Means to Promote Consumer Interests and Public Welfare – An Introduction* in *German Federal Ministry of Justice and Consumer Protection,* Max Planck Institute for Innovation and Competition (eds.), Data Access, Consumer Interests and Public Welfare, Baden-Baden 2021, 11 ss.

[17] European Commission, Final Report from the Commission to the Council and the European Parliament – *Final report – sector inquiry into consumer Internet of Things*.

[18] 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).

[19] 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).

cy for Cybersecurity (ENISA).

- The proposal for a Cyber Resilience Act[20], which aims at harmonising cybersecurity rules for products with digital elements, therefore tackling Internet of Things products specifically.

- A new framework on civil liability:
  In this context the Union looked at Artificial Intelligence, IoT and robotics together, as they share some main characteristics that have led the European legislator to combine the analyses and legislative interventions. The framework represents a package of legal actions with the purpose of raising trust towards AI-related products at the Union level and ensuring that remedies and actions for damages are accessible to final consumers. The framework includes:
  - The proposal for an AI Liability Directive[21], aiming at adapting non-contractual civil liability rules to artificial intelligence.
  - The proposal for a renewed Product Liability Directive[22], dealing with liability for defective products: in the proposal the scope of the Directive has been extended to include digital products and it considers them within the context of circular economy, expanding the responsibility of manufacturers.
- The Ecodesign and Energy Labelling – Framework Directives[23], two Directives tackling energy-using products (EUPs), among which it is possible to classify Internet of Things products. The Framework is addressed to highlight some information requisites placed on manufacturers.

2. European legislative initiatives to regulate the Internet of Things

2.1. Governance and Strategy

IoT data governance can be challenging as Internet of Things devices involve different kind of data: personal data of the final user (which are protected by the provisions of the General Data Protection Regulation) and non-personal data, that are generated by the very use of the device[24]. These data mainly remain in control of the manufac-

[20] European Commission, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act).

[21] European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).

[22] European Commission, Proposal for a Directive of the European Parliament and the Council on liability for defective products, (Product Liability Directive).

[23] The Framework comprehends: Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products; Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU.

[24] W. Kerber, *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, in *GRUR International*, 2023, 72(2), 120 ss.

turer who designed the product, usually giving little to no access to consumers to the generated information.

2.1.1. The Data Act

The proposal for a Regulation on harmonised rules on fair access to and use of data was adopted by the Commission on February 23rd, 2022, and it marks a fundamental pillar of the Digital Decade.[25] It is set to bring fairness into the technological perspectives by setting up provisions on how to use and process data generated by Internet of Things Devices.

The Proposal introduces:

- «Measures to allow users of connected devices to gain access to data generated by them […]; and to share such data with third parties to provide aftermarket or other data-driven innovative services. It maintains incentives for manufacturers to continue investing in high-quality data generation, by covering their transfer-related costs and excluding use of shared data in direct competition with their product.
- Measures to rebalance negotiation power for SMEs by preventing abuse of contractual imbalances in data sharing contracts. […]
- Means for public sector bodies to access and use data held by the private sector that is necessary for exceptional circumstances, particularly in case of a public emergency […]
- New rules allowing customers to effectively switch between different cloud data-processing services providers and putting in place safeguards against unlawful data transfer»[26].

On December 2022 a compromise text was discussed by the EU Council, extending its entry into application from the original 12 months to 18 months.[27] The transition in the past months within the EU Council from the Czech presidency to the Swedish presidency, to the Spanish presidency seems to have enhanced the urgency of the document, making it a priority.[28] In mid-March the European Parliament's voted in plenary session to approve their version of the Data Act, opening the door to interinstitutional discussions with the EU Council and Commission. In June 2023 a political agreement was reached on the document. Significant proposals have been introduced to increase transparency for the manufacturers and to regulate B2B data transfers.[29] The new rules are awaited with some excitement by Member States as they shall create and additional GDPR of €270 billion by 2028 by tackling the legal, economic and

[25] European Commission, *Shaping's Europe Digital Future – Data Act*.

[26] European Commission, *Press Release - Data Act: Commission proposes measures for a fair and innovative data economy*, 23 February 2022, available at *ec.europa.eu*.

[27] L. Bertuzzi, *EU Council set to revise cloud-related provisions in new data law*, in *EURACTIV*, 9 December 2022 (updated on 13th December 2022), available at *euractiv.com*.

[28] L. Bertuzzi, *Swedish presidency offers EU countries options on Data Act's pain points*, in *EURACTIV*, 12 January 2023 (updated on 13th January 2023), available at *euractiv.com*

[29] L. Bertuzzi, *EU lawmakers formalise position on the Data Act in plenary vote*, in *EURACTIV*, 14 March 2023 (updated on 16th March 2023), available at *euractiv.com*.

technical reasons that lead to a limited use of some data.[30]

The proposal is consistent with existing rules on the use of personal data (addressed by the General Data Protection Regulation[31]) and non-personal data (regulated by the Free Flow of Non-Personal Data Regulation[32]), but also with Competition law in the context of data sharing, the Database Directive[33] and the Open Data Directive[34]. Among the most recent texts it takes into considerations also the propositions of the Data Governance Act[35] and it complements the Digital Market Act.[36]

Within this kaleidoscopic set of rules, the Data Act shows a high level of consumer protection, addressing the difficulties that final users usually have in gaining access to information generated by IoT devices; due both to their high technicalities and to a not-always adequate level of consciousness showed by companies. The proposal aims at «further empowering consumers using products or related services to meaningfully control how the data generated by their use of the product or related service is used»[37]. By doing so it imposes a consequent burden on manufacturers as it obliges the data holder to make data available[38] and to transfer them when requested[39] (a sort of "extended right to access" and an "extended right to data portability"). The manufacturers can still access data and use them, but they «would have to design their products in a way that allows the user to access the generated data easily by default and be transparent on what data will be accessible and how to access them»[40]. In the last political agreement, it was better defined the scope of the obligation which will cover intentional and indirect actions and data used and generated in standby mode. As it is still unclear if it will cover organisations based outside the EU, it has been decided that data shall be anonymized and will have to occur in a standardised and real-time manner. [41]

This approach somehow follows the footsteps of the General Data Protection Reg-

[30] European Commission, *Press Release - Data Act.*

[31] 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).

[32] 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.

[33] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of database.

[34] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

[35] European Commission, Proposal for a Regulation of the European parliament and of the Council on European data governance (Data Governance Act).

[36] European Commission, Proposal for a Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data (Data Act).

[37] European Commission, Proposal for Data Act, Explanatory Memorandum, 13.

[38] European Commission, Proposal for Data Act, Chapter III.

[39] European Commission, Proposal for Data Act, Chapter VI.

[40] European Parliamentary Research Service (EPRS), *Briefing – The Data act,* 5 October 2022, available at *europarl.europa.eu*.

[41] L. Bertuzzi, *Data Act: EU institutions finalise agreement on industrial data law*, in *EURACTIV*, 28 June 2023 (updated on 30th June 2023), available at *euractiv.com*.

ulation (for example, by adopting by design and by default principles) and it widens its approach into a more comprehensive requirement of "data management", where data are governed in a user-centric way and therefore explainability, transparency and availability of data must be persistent in every product and service dealing with data.
It shall be noted that the burden imposed on companies might be relieved a little by presuming a compensation for making data available, which shall be «reasonable and agreed with the data recipient».[42] It makes sense as proper and functioning data accesses mechanisms require multi-sector investments in data quality, processes and technical arrangements; as long as data holders may not hinder access to data (or make it too difficult) trying to obtain a remuneration in exchange for information that shall (at least in part) be easily accessible.[43]
Scholars have been given some opinions on the Act, stressing its necessity (and urgency) but also drawing attention to some limits of the proposal. Wolfgang Kerber[44], Professor of Economics at the Marburg University, in Germany, underlines that even though market necessities surrounding the Internet of Things have, indeed, been listed correctly by the Act, there is still a lot of work to do. First, the mechanisms to enforce user right to access still seem to weak to be effective (due to «insufficient scope of data, lacking technical interoperability, high transaction costs, esp. through the need for a negotiated contract with FRAND conditions, unclarity regarding data markets»[45]), second (and extremely relevant for our purposes) the attempt to make user regain control over his/her data «will not work due to unsolved serious market failure problems in B2C situations, i.e. that all the rights to use the IoT data will end up with the data holders (and leave the consumers with only these weak user rights)».[46]
A Data Act is needed, as a huge portion of the market needs regulation, and although it cannot be excluded that some rebalances might be necessary and may be considered in the following steps of the decision process; some adjustments within business processes and consumer-relationships may come in handy to solve (at least partly) some concerns, as it will further be analyzed in the last section of this paper.

2.2. Cybersecurity

The European legislator is investing its resources in enhancing the dedicated cybersecurity landscape, a key component in the development of connected technologies as well as a priority of the Digital Decade, as «cybersecurity is an integral part of Europeans' security. Whether it is connected devices, electricity grids, or banks, aircraft, public administrations, or hospitals they use or frequent, people deserve to do so within the assurance that they will be shielded from cyber threats. The EU's economy,

42 EPRS, *Briefing – The Data act*, p.6(f).

43 J. Drexl, *Data access as a means to promote consumer interests and public welfare – An introduction*, cit., 21.

44 W. Kerber, *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, in *GRUR International*, 2022.

45 Ivi, 1.

46 *Ibidem.*

democracy and society depend more than ever on secure and reliable digital tools and connectivity. Cybersecurity is therefore essential for building a resilient, green, and digital Europe».[47]

Threats to cyber safety are real and increasing: in the tenth edition of the ENISA Threat Landscape (ETL) report[48] among the key trends in cyber threats the Agency affirmed that «DDoS [have been identified for] getting larger and more complex, are moving towards mobile networks and IoT and are being used in the context of cyber-warfare».[49] And «IoT malware has increased over 2021. The change in the first half of 2022 shows the prevalence of IoT targeting malware almost doubling. In the first 6 months of 2022, the attack volume is already higher than had been recorded over the last 4 year»[50].

A multi-front approach[51] has been adopted by European institutions which resulted in a prolific production of cybersecurity provisions devoted to cover specific and diverse aspects of technological security.[52]

In 2013 the Directive on Attacks against Information Systems came into force, aiming at harmonising criminal offences related to information systems. In 2016 the Directive on Security and Information Systems (also known as the NIS Directive) tackled critical infrastructures; replaced on December 2022 by the NIS2 Directive, which broadens the scope the first Directive improving cybersecurity risk management and introducing reporting obligations across strategic sectors (e.g. energy, transport, health and digital infrastructure). Other sectoral legislations adopted are the Directive on the Resilience of Critical Entities (CER) which aims to reduce the cyber vulnerabilities and strengthen the resilience of entities providing essential services that are crucial for the maintenance of vital societal functions, economic activities, public health and safety, and the environment (so-called critical entities);[53] and the DORA Regulation (Regulation on Operational Resilience of the Financial Sector), which "sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics service."[54]

---

[47] European Commission, *Joint Communication to The European Parliament and the Council on the EU's Cybersecurity Strategy for the Digital Decade.*

[48] As explained in the ENISA website, the ETL is «an annual report on the status of the cybersecurity threat landscape. It identifies the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis. It also describes relevant mitigation measures».

[49] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape (ETL) Report,* 2022, 11.

[50] Ivi, 50.

[51] P. G. Chiara, *The IoT and the new EU cybersecurity regulatory landscape*, in *International Review of Law, Computers & Technology*, 2022, 118-137.

[52] EPRS, *Briefing EU Legislation in progress "EU cyber-resilience act",* December 2022.

[53] European Commission, *Critical Infrastructure: Commission accelerates work to build up European resilience*, 2022, 18, available at *ec.europa.eu.*

[54] European Council, Press Release: *Digital finance: Council adopts Digital Operational Resilience Act*, 2022, 28, available at *consilium.europa.eu.*

To widen the already broad legal landscape two more instruments have been introduced, specifically designed to assess cybersecurity in relation with connected devices:

- The rsecurity Act, introducing a cybersecurity certification scheme made in Europe.

Such a strong effort on behalf of the European Union is justified as «the absence of a cybersecurity legal framework for product with digital elements incentivises the development of potentially diverging national rules among Member States, threatening an open and competitive single market».[55] A matter that becomes even more urgent with the rising of interoperability protocols which by expanding the possibility of sharing data also increase opportunities for threats and malicious attacks.

2.2.1. The Cyber Resilience Act (CRA)

The proposal, based on the provisions of Article 114 TFUE, is a horizontal piece of legislation with the purpose of harmonizing cybersecurity rules on products with digital elements[56] not covered by any previous regulation, seeking to establish a common ground of cybersecurity rules, ensuring more secure hardware and software products. The CRA imposes a burden on manufacturers who must ensure compliance with European cybersecurity requirements. Products will be subjected to a conformity assessment, and the procedure may vary based on the degree of criticality of the product. The Spanish presidency of the EU Council of Ministers released a fine-tuned version of the text at the beginning of July 2023.[57] The last version of the document obliges manufacturers that become aware of incidents or vulnerabilities to actively inform the competent authority. The task of evaluating the reports has been put in the hands of the national Computer Security Incident Response Teams (CSIRTs) relieving the ENISA from the task which will have to manage a pan-European platform to analyse complementarities and establish a vulnerabilities database.

The proposal used to divide products with digital elements into two categories[58] (as better shown in Figure 1):

- Default non-critical products (like smart home assistants).

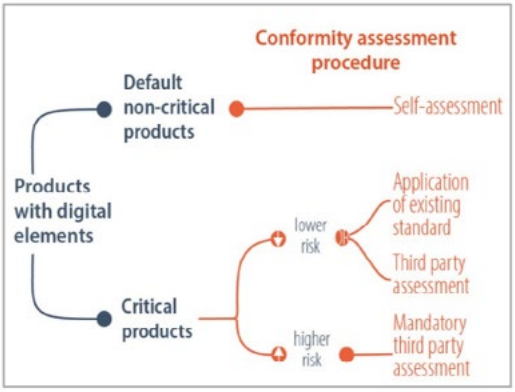


Figure 1. Cyber resilience conformity assessment, Source: EPRS, EU cyber-resilience act – Briefing

[55] EPRS, *Briefing EU Legislation in progress – EU cyber-resilience act*, 2022, 3.

[56] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020* (Cyber Resilience Act).

[57] L. Bertuzzi, *EU ambassadors set to endorse new cybersecurity law for connected devices*, in *EURACTIV*, 2023, available at *euractiv.com*.

[58] EPRS, *Briefing EU Legislation in progress "EU cyber-resilience act"*, 2022, available at *europarl.europa.eu*.

- Critical products, which are further divided into products carrying a higher or lower risk.

However, the last version of the text[59] removed any explicit reference to "highly critical products" and specific assurance level requirements replacing it with a first list of highly critical products categories and the obligation to conduct an impact assessment «to assess the supply and demand side of the internal market and the capability and readiness of the member states for the schemes' implementation»[60] before asking for any mandatory certifications.

Cybersecurity is imperative: the EU is clearly putting an effort to assure that companies and manufacturers are on board with the commitment to ensure a safer experience to their consumers. Therefore, it imposes significant fines on manufacturers who may not follow the given requirements: they might risk 15 million fine or 2.5% of their annual turnover worldwide for non-compliance with the security requirements and/or a 10 million fine or 2% of their total annual turnover worldwide for lack of compliance with all other obligations in the regulation.

The legislative process is still ongoing. The last Swedish presidency of the EU Council suggested three partial compromises to the old text[61] and the Spanish presidency is now working on the text. Among the introductions a couple have an interesting side effect. First, manufacturers must state a potential product lifespan during which customers will receive security updates. Second, it is the economic operators who significantly impact connected devices who are now responsible for adhering to the cybersecurity rules. The introduction of security updates that do not alter a product's intended use actually exempts the creator from this liability. These specifications wave somehow the burden on manufacturers which, righty exists but tries to not exceed the perimeter of doable interventions.

2.2.2. The Cybersecurity Act

The Cybersecurity Act entered into force in June 2019. The document focused on the position of the European Union Agency for Cybersecurity (ENISA) and on the adoption of a European cybersecurity certification.

Thanks to the provisions of the Cybersecurity Act the Agency was granted a permanent mandate and saw an overall enhancement of its role in supporting the Union to achieve a common and high-level cybersecurity. For our purposes, the Act finds its main relevance in the creation of a European cybersecurity certification scheme: a comprehensive set of rules, technical requirements, standards, and procedures agreed at European level for the evaluation of the cybersecurity characteristics of a specific

[59] L. Bertuzzi, *Data Act: EU institutions finalise agreement on industrial data law*, cit.

[60] L. Bertuzzi, *EU ambassadors set to endorse new cybersecurity law for connected devices,* cit.

[61] Among the main suggestions, two further crucial conditions were imposed: first, each linked device needs a special product identifier to enable identification and security patches shall easily identify the applicability of security updates. Second, in order to dispose of a product securely, the text now mandates that the manufacturers provide users with the ability to safely and easily erase all data and settings, including those permitting access to Wi-Fi networks, from the product.

product, service, or process. The project is laudable, and a single certification recognized throughout Europe and validated by a European agency would certainly lend homogeneity to an ever-changing landscape. However, the adoption of the certification scheme is still on a voluntary basis, and this partially nullifies the positives of the initiative. Cybersecurity initiatives, especially in the IoT sector, are definitely supported and promoted at national level (the Finnish Cybersecurity Label proposed by the Finnish Transport and Communications Agency[62] is a perfect example), however a proliferation of certifications may lead to "legal fragmentation in the Single Market"[63] and a common cybersecurity certification scheme (even better if specifically tackling IoT) will definitely help to reach clarity and harmonization.
It shall be noted that the European Union is not the only entity to increase its efforts on preserving the safety of the digital scene. The Organization for Economic Co-operation and Development (OECD) in its Policy Framework on Digital Security published on December 2022 states that «digital security is a means to achieve economic and social objectives rather than an end it itself. Therefore, it is important to design and implement digital security policies that are consistent with those developed in other related policy areas. When designed and/or implemented in isolation, digital security policies are likely to be inconsistent with other policy areas, and to be perceived as burdensome, costly, and counterproductive. When they aim at creating synergies with other policy areas' objectives, digital security policies are likely to be more effective[64]».

2.3. Liability

IoT devices can challenge the traditional notions of civil liability,[65] therefore at the EU level many resources are being invested in assuring that Artificial Intelligence and mechanisms built on AI or integrated with AI systems can be trusted.[66]
When dealing with civil liability the Union does not look at IoT distinctively from AI, but in this context considers AI, IoT and robotics as opportunities to be looked at together, as they all «can combine connectivity, autonomy and data dependency to perform tasks with little or no human control or supervision. […] Their complexity is reflected in both the plurality of economic operators involved […] and the multiplicity of components […]. Added to this is the openness to updates and upgrades after their placement on the market. The vast amount of data involved, the reliance

[62] Finnish Transport and Communications Agency, *Finnish Cybersecurity Label*, 2020, available at: *tietoturvamerkki.fi*.

[63] P.G. Chiara, *The IoT and the new EU cybersecurity regulatory landscape*, in *International Review of Law, Computers & Technology,* 2022, 6.

[64] Organization for Economic Co-operation and Development (OECD), *OECD Policy Framework on Digital Security Cybersecurity for Prosperity*, 2022, 9, available at *oecd.org*.

[65] L. E. Gorman, *The Era of the Internet of Things: Can Product Liability Laws Keep Up?,* in *Defense Counsel Journal*, 84, 2017, 215.

[66] 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*, Brussels, 8 April 2019.

on algorithms and the opacity of AI decision-making, make it more difficult to predict the behaviour of an AI-enabled product and to understand the potential causes of a damage. Finally, connectivity and openness can also expose AI and IoT products to cyber-threats».[67]

AI, IoT and robotics represent a chance not to be missed for Europe. In order to maintain a relevant role in the global discussion tables on new technologies, the EU needs not only to make strategic choices (which is one of the main purposes of the Data Act) and impose common technical requirements (plumping up the cybersecurity framework is definitely a step in this direction), but also to hearten its citizens that products and services with digital elements that respond to digital logics are reliable and, whenever necessary, bring with them at least the same remedies as non-digital products. To reduce the degree of uncertainty and to support the commercial objectives underlying the European Digital Decade, the Commission takes into its own hands the task of guaranteeing a high degree of protection to its citizens and it proposes two Directives: the so-called AI Liability Directive[68] and a renewal of the already existing Product Liability Directive.[69]

The Commission assumes a holistic approach: «[t]hese two policy initiatives are closely linked and form a package, as claims falling within their scope deal with different types of liability. The Product Liability Directive covers producer's no-fault liability for defective products, leading to compensation for certain types of damages, mainly suffered by individuals. [The AI Liability Directive] covers national liability claims mainly based on the fault of any person with a view of compensating any type of damage and any type of victim. They complement one another to form an overall effective civil liability system».[70]

2.3.1. AI Liability Directive

Technologies based on AI are intrinsically complex, autonomous, and not always as transparent, therefore users may struggle to understand the underlying logic.[71] Civil liability must ensure victims the opportunity to claim for compensation and a real shot at fair trial,[72] making the claim process accessible. In the eyes of the Union this type

[67] 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 of Artificial Intelligence, the Internet of Things and robotics*, Brussels, 2020, 2.

[68] European Commission, *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence* (AI Liability Directive).

[69] European Commission, *Proposal for a Directive of the European Parliament and of the Council on liability for defective products.*

[70] European Commission, *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence* (AI Liability Directive).

[71] They are generally defined "black-boxes", to which are opposed efforts made by scholars and technicians to make the AI "explainable" – on the topic please see: K. K. Chennan et al, *Black Box Model for Explainable Artificial Intelligence*, in M. Metha et al. (eds.), *Explainable AI: Foundations, Methodologies and Applications,* Intelligent Systems Reference Library Volume 232, New York City, 2023, 1 ss.

[72] Art. 47, Charter of Fundamental Rights: «Everyone whose rights and freedoms ranteed

of goal is better addressed at supranational level, in order to avoid rules fragmentation and uncertainty[73] that may come from a merely national approach. The Directive aims at providing a solid basis for compensation to damages caused by AI-systems (eventually in the lack of compliance with national or Union law) and it establishes a "targeted rebuttable presumption of casualty"[74]: a presumption of causal link, which eases the process of causal link identification. This represents a needed support especially in cases where AI are designed as black boxes[75] and are therefore difficult to decipher.
The AI Liability Directive does not directly address Internet of Things products, however, it is relevant for our purposes in that it provides an overall protective framework for the consumer to access remedies and contributes to the creation of a safe and defined legal landscape, positioning itself in accordance with the AI Act, to which it makes repeated references. In fact, even though it cannot used by itself to start a lawsuit under certain conditions can reverse the burden of proof.
The work on the AI Liability Directive is strictly connected to the AI Act, it has been put aside waiting for the final text of the AI Regulation.

2.3.2. Product Liability Directive (PLD)

The proposal for a revision of the Product Liability Directive together with the proposal for the adoption of an AI Liability Directive generate a package of complementary legal instruments, sharing the common goal of adjusting liability to the digital age and AI systems.
The renewal of the Directive takes into consideration a pool of regulations that swings from protection of consumers,[76] to personal data protection, to damages connected with environmental issues. Moreover, references to the Cybersecurity initiatives[77] and other legislative sector-specific[78] rules help assuring a safety framework for products in the EU internal market. Among them, constant referrals to the AI Act (which hopefully will provide some underlying requirements and definitions) promises a general

by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice».

73 Even though the chosen legal instrument to rule on the matter is a "Directive" which leaves some leeway to Member States to implement rules in their own national systems.

74 European Commission, *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence* (AI Liability Directive), 2022, 13.

75 Please see note 71 for some further references.

76 For example, the Sale of Goods Act and the Digital Content and Service Directive, that deal with consumer protection concerning contractual liability.

77 The Cybersecurity Act and the Cyber-resilience Act, which aim at mitigating cyber-threats while imposing obligations on manufacturers, although they do not specifically address liability.

78 Such as the Machinery Regulation, the proposed General Product Safety Regulation and even the recently adopted Digital Service Act. They do not concern liability issues and responses.

harmonization among the new provisions and it confirms that AI systems and AI-enabled goods indeed fall within the scope of the renewed Directive[79], extending the possibility of compensation also to IoT Products and services, including not only manufacturers of hardware products but also providers of software and digital services.[80] «The PLD proposal will ensure that when AI Systems are defective and cause physical harm, property damage or data loss it is possible to seek compensation from the AI-System provider or from any manufacturer that integrates an AI system into another product».[81] The Directive stipulates that in some specified situations when these are too complicated for the defendant to prove, notably due to technological or scientific complexity, national courts may presume the defectiveness of a product or a causal connection between the damage and the fault. In addition, an economic operator may be exempt from liability if it can show that the defects of the product were not apparent at the time due to the state of science and technology at the time.

At the beginning of March 2023, a draft on the updated Product Liability Directive was presented by Swedish chair of the EU Council. It defines more explicitly the term "manufacturer's control" and aims at reducing national fragmentation on the topic. The text has been updated to reflect a non-paper from the European Commission that made it clear that software, including that offered through "as-a-service" model, like Netflix or Microsoft 365, is a product and therefore is covered by the Act. Similarly, in the March version of the text the associated digital services that are built into or connected to the product have been better defined as, for example, traffic information for a navigation system or a temperature control service that monitors the operation of a smart fridge.[82]

However, one of the last acts of the Swedish presidency, before leaving the chair to the Spanish presidency, was to circulate e new compromise text on the proposal in late May 2023. The last draft law indicates that open software provided for free and outside a commercial activity is excluded from the scope of the liability rules. The text also clarifies that if a manufacturer integrates the open-source software as a component of its product and it consequently causes a defect, the liability will then fall on the

[79] This answers the call for the European Parliament made in 2020: European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence.

[80] Recital 12 of the Product Liability Directive: «Products in the digital age can be tangible or intangible. Software, such as operating systems, firmware, computer programs, applications, or AI systems, is increasingly common on the market and plays an increasingly important role for product safety. Software is capable of being placed on the market as a standalone product and may subsequently be integrated into other products as a component, and is capable of causing damage through its execution. In the interest of legal certainty, it should therefore be clarified that software is a product for the purposes of applying no-fault liability, irrespective of the mode of its supply or usage, and therefore irrespective of whether the software is stored on a device or accessed through cloud technologies. The source code of software, however, is not to be considered as a product for the purposes of this Directive as this is pure information. The developer or producer of software, including AI system providers within the meaning of [Regulation (EU) …/… (AI Act)], should be treated as a manufacturer».

[81] European Commission, Proposal for a Directive of the European Parliament and the Council on liability for defective products, 2022.

[82] L. Bertuzzi, *EU Council refines scope, responsibilities in product liability rulebook*, in *EURACTIV*, 2023, available at *euractiv.com*.

manufacturer rather than the software provider. It is interesting to notice a turnaround compared to March: the EU Council made it clear that internet access services should not be regarded as services products and are therefore not covered by the Directive. In addition, if a product depends on internet connectivity to maintain security and loses connectivity, it will be regarded as defective. This specification is especially crucial for Internet of Things (IoT) products in light of the impending Cyber Resilience Act, which will mandate the enrolment of security fixes over a certain period of time. [83]
Given the history of the PLD, it suffers less its connection with the AI Act: although it exists a Product Liability Directive has been in place since 1985 therefore the work on the document it is sped up compared to the AI Liability Directive. Although there is still space of manoeuvre for change of plans «the co-rapporteurs are pushing on the accelerator to reach a committee-level agreement by September, with bilateral meeting with political groups already kicking off».[84]

2.3.2.1. Circular Economy

The renewed Productive Liability Directive reflects the context of the so-called "circular economy", the EU action plan adopted on March 2020.[85] Generally speaking, a «circular economy is an economic system designed with the intention that maximum use is extracted from resources and minimum waste is generated for disposal».[86] For the business model designed by it, products that are able, through their internet connection, to be modified and/or upgraded to enhance their productivity or to elongate their lifespan are part of the circular economy.[87] In fact, «[i]t is becoming increasingly common for digital services to be integrated in or interconnected with a product in such a way that the absence of the service would prevent the product from performing one of its functions, for example the continuous supply of traffic data in a navigation system. While [The Product Liability] Directive should not apply to services as such, it is necessary to extend no-fault liability to such digital services as they determine the safety of the product just as much as physical or digital components. Such related services should be considered as components of the product to which they are inter-connected, when they are within the control of the manufacturer of that product, in the sense that they are supplied by the manufacturer itself or that the manufacturer

[83] L. Bertuzzi, *EU Council closes in on product liability rulebook,* in *EURACTIV*, 2023, available at *euractiv.com.*

[84] L. Bertuzzi – M. Killeen, *The product liability train, the Commission's AI guidelines*, in *EURACTIV*, 2 June 2023, available at *euractive.com.*

[85] It is one of the main steps of the European Green Deal, for more information please see the dedicated area on the European Commission Website, *Circular economy action plan,* available at *environment.ec.europa.eu.*

[86] P. Deutz, *Circular Economy*, *International Encyclopedia of Human Geography*, 2020, 193 ss., available at: *sciencedirect.com.*

[87] Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999.

recommends them or otherwise influences their supply by a third party».[88]
However, this also means imposing on manufacturers an obligation to extend their efforts over the products even after the go-to market moment. Indeed, art. 6.1(e) of the revised Directive expands temporally the scope of responsibility of the manufacturer extending it to after the placement of the product on the market. The Article states that:
«1. A product shall be considered defective when it does not provide the safety which the public at large is entitled to expect, taking all circumstances into account, including the following: […]
(e) the moment in time when the product was placed on the market or put into service or, where the manufacturer retains control over the product after that moment, the moment in time when the product left the control of the manufacturer».
According to Article 6 the manufacturer must continue to exercise a certain degree of control over the product even when it is on the market, and it is used by consumers. This control resolves in the obligation to update the product (and its software) and be aware that this operation must be extended to all products able to support it. Furthermore, Recital 37 states that «since digital technologies allow manufacturers to exercise control beyond the moment of placing the product on the market or putting into service, manufacturers should remain liable for defectiveness that comes into being after that moment as a result of software or related services within their control, be it in the form of upgrades or updates or machine-learning algorithms».
These provisions impose on the manufacturer a sort of *de facto* obligation to update or upgrade products, which is particularly relevant when dealing with IoT products that usually undergo a periodical revision process which may easily lead to updates and upgrades.

2.3.2.2. Creating a communication channel with consumers

Usually, consumers are informed of updates as they must take positive actions to physically upgrade the connected appliances. Updates are mainly communicated via push notifications or similar messages, that inform the user that a new version of a software is ready to be installed. The exchange of information results in the creation of a communication channel with the consumer, who gets use to receiving messages from the manufacturer and expects his/her service or product to get better with time (and with the technological advancements). This scenario even creates an expectation in customers to receive communication regarding ameliorations to a certain product or service. At the same time manufacturers have all the interest in users downloading the last version of their technology as through its use they can get feedback and improving their offers even more, better targeting the interest of their consumers. It seems that the PDL (and in some ways even the previous acts analysed) are building the ground for this communication channel to become fundamental, and frequently used.

[88] Product Liability Directive, Recital 15.

A legislative imposition to frequent exchanges with consumers is no news to manufacturers: for example, when dealing with products that consume energy (the so-called energy-using products (EUPs), among which it is also possible to classify Internet of Things) the Ecodesign and Energy Labelling – Framework Directives impose to manufacturers specific[89] and generic requirements[90] which «may entail information requirements, such as material provided by the manufacturer about best practices to use and maintain the product to minimise its environmental impact. [Moreover] it may require that the manufacturer perform a lifecycle analysis of the product to identify alternative design options and solutions for improvement».[91]

Therefore, it seems that manufacturers of energy-consuming products that fall within the scope of the product liability directive shall endeavour to build their communication channel in a transparent manner, structuring the information efficiently enough that it is quickly transposable and suitable for the understanding of end-consumers.

3. Using IoT technology means establishing a relationship with consumers

At the beginning of 2022 the European Commission released a report on a sector inquiry into consumer Internet of Things.[92] The report stated that «in relation to data use cases within consumer IoT companies, respondents [i.e., Businesses involving IoT products and/or services] report that they use the data collected for:

1. the normal functioning of consumer IoT products and services;
2. the personalisation of the user experience;
3. business analytics;
4. product maintenance and development;
5. various other use cases (for example marketing communication, safety and fraud prevention)».[93]

The respondents also pointed out the cost of technology investments and the effort required to be part of the market of the IoT technologies.[94] To be competitive in the IoT sector, technical fundings are accompanied by efforts and investments aimed at preserving data protection rights and answering requests by consumers connected to the use of data. Lately the EU current legislative landscape seems to stress in particular the right to access data and the right to data portability. Especially with the entry onto force of the Data Act these rights will definitely need to be reinforced within

[89] For example, to set limit values to the maximum energy consumption or minimum quantities of recycled material.

[90] For example, that a product is "energy efficient" or "recyclable" (please note that compliance with the relevant harmonised European standard, gives presumption of conformity with the requirement).

[91] European Commission, *Ecodesign your Future – how Ecodesign can help the environment by making products smarter*, 2014, available at *op.europa.eu*.

[92] European Commission, Final Report from the Commission to the Council and the European Parliament, *Final report – sector inquiry into consumer Internet of Things*, 2022.

[93] Ivi, 37.

[94] Ivi, 13.

companies.
It seems that manufacturers of products and services IoT-related are being pushed to put more effort in the way they build and maintain the communication channel with their customers, as the information that are being asked to provide are increasing with the evolving European legal landscape. End-consumers need to be empowered to access their own data (this already as provided by the GDPR and in future also on the basis of the Data Act), to know the security mechanisms related to the connected device they are using (in different ways this is asked both by the GDPR and Cybersecurity initiatives), to receive information about a more energetically conscious use of their products (as requested by the Ecodesign Directives), and to have all the information they need to ask for remedies in case of damages (as stated in the Product Liability Directive).
To further extend the number of information given, along with these requirements also come the protections (and related communications) dictated by provisions on consumer protection.

3.1. Consumer protection

In Spring 2020 the Commission launched the so-called «Fitness Check of EU consumer law on digital fairness [to] determine whether the existing key horizontal consumer law instruments remain adequate for ensuring a high level of consumer protection in the digital environment».[95]
Among other initiatives one that aims at updating consumer protection and keeping it up to date to market requests and changes is the New Deal for Consumers, adopted on April 2022 and as part of the New Deal on 27 November 2019 it was adopted the Directive on better enforcement and modernization of EU consumer protection.[96] The Directive, also known as the "Omnibus Directive" suggested updates to other Directives[97] and while aiming for a general higher degree of transparency in purchases on the digital market (for example asking for clear indications of whether the seller is a professional or not and on who is responsible for deliveries), and for enhanced rights regarding processing of personal data (e.g. right to access and withdrawal period);[98] it also imposed an obligation to inform consumers «about how offers are ranked in search results and identify paid advertisements»[99] and about price changes on specific

[95] European Commission, *Review of EU consumer law*, available at *commission.europa.eu*.

[96] Member States were called to transpose the new rules in their systems by the end of November 2021 and rules should have become effective by May 2022. However, not all Member States have done the necessary activities yet.

[97] Directives involved are: The Unfair Commercial Practices Directive (2005/29/EC); The Unfair Contract Terms Directive (93/13/EEC); The Consumer Rights Directive (2011/83/EU); The Price Indications Directive (98/6/EC).

[98] Other provisions refer to ensuring that price reduction claims are genuine, that remedies against harm are effective or that reviews can be certified.

[99] European Commission, Factsheet, *New Consumer rights – what benefits will I get?*, 2022, available at *commission.europa.eu*.

offers, so «that they are aware of the risk that the asking price was increased».[100]
The Omnibus Directive seems to be fitted to be part of the general approach suggesting more attentive, transparent, and frequent conversations with consumers, who shall be constantly informed of changes and given the necessary instruments to understand the internal market and its movements.

4. Conclusions: marketing communications and legal information may share some purposes

Attempting at drawing together the provisions analysed, a few considerations can be made.
First, entering the IoT market as a responsible manufacturer requires investments on multi and different levels and many proposed legislations will force companies to allocate resources on different areas of their businesses to legally and safely produce and market IoT devices and/or IoT-related services.
Second, the provisions analysed set out a general imposition (or at least a strong suggestion) to communicate with customers in an understandable and consistent way, which (again) requires studies, investments, resources and attention to create products and services that are transparent and explicable by design but also to build a structure able to answer the requests of consumers.
Third, usually there are limitations to the time a business can use data related to its customers for commercial purposes (for example for marketing activities or campaigns). Entities are requested to ask for consent and when the time validity of the given consent has expired communications shall stop and data must be erased. A specific opinion of the Italian Data Protection Supervisory Authority states that: «[a]t all events, the detailed data on the items purchased by identifiable customers may be retained for profiling or marketing purposes for no longer than twelve or twenty-four months, respectively, as of their storage, subject to their being actually anonymised in such a way as to prevent data subjects from being identified also indirectly and/or via interconnections with other databases». Some exceptions have been suggested by the same Authority when dealing with luxury goods[101], although underlying that for other type of products the limit of the validity of consent for marketing purposes is 24 months.[102]
Manufacturers will be torn between information that are or will be obliged to give (in-

[100] *Ibidem.*

[101] Garante Privacy, "*Fidelity card" e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione*, 24 febbraio 2005 (doc. web 1103045).

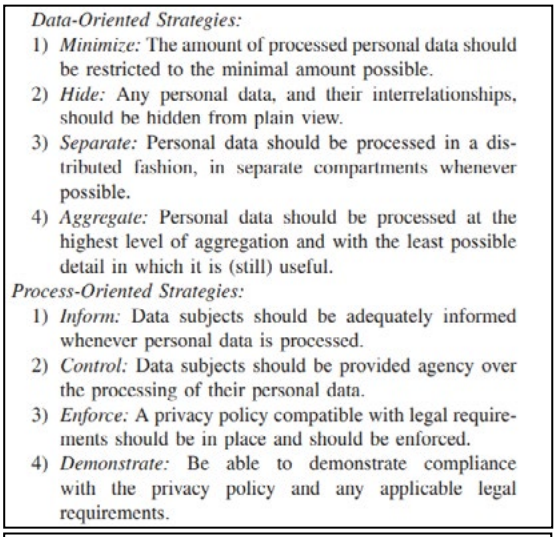
[102] Relevant provisions on the matter, all by the Italian Data Protection Supervisory Authority are: Garante Privacy, *Verifica preliminare. Prolungamento dei tempi di conservazione dei dati personali riferiti alla clientela per il loro utilizzo a fini di profilazione e di promozione commerciale profilata*, 18 aprile 2018 (doc. web 8997404); Garante Privacy, *Verifica preliminare. Trattamento di dati personali riferiti alla clientela per finalità di profilazione e promozionale*, 5 luglio 2017 (doc. web 6844421); Garante Privacy, *Trattamento e conservazione di dati personali della clientela per finalità di profilazione. Verifica preliminare richiesta da Bulgari S.p.A.,* 24 aprile 2013 (doc. web 2499354).

formation contained in the privacy policy, changes in the processing of data,[103] ways to make your device more energetically efficient, safety measures…etc) and information that they economically benefit form, like communications related to marketing actions and campaigns. Moreover, even though not all information requires to the same economical investments, if the sanctions usually implied to lack of compliant with the EU provisions and/or the loss of profits when marketing communications are shut down are to be considered, the commercial and economic implications related to the establishment and management of a communication channel with consumers are relevant.
Fourth, as many studies showed[104] consumers are not very keen to be slowed down by communications given by providers or manufacturers and their attention to additional information are limited to a short time frame.
Fifth, as said, connected devices (such as smart home appliances) use and generate a huge quantity of data, both personal and non-personal, a characteristic that is intrinsic in the nature of the IoT technology. Data generated and collected create patterns based on the everyday life of consumers. This strong connection with habits of consumers is what makes a service or a product efficient, but it also makes it dependent to a continuous flow of data, which must be governed in a responsible way by data holders.
From these observations, it seems that when it comes to IoT-related products and services, there are different types of information that overlap with each other but have one final recipient: the consumer.
Manufacturers are required to disentangle different standards, keeping in mind that communications must be simple, effective, reliable and, for them to also be economically feasible, as standard as possible. Therefore, a responsible attitude in this regard could be precisely to create a single communication channel, which may have different layers of security and types of information given, segmented and composable, and which allows to prolong a type of communication that is clear and does not confuse the user.
It may be based on a granular and transparent consent, easier to govern and compliant with different security standards based on the different kind of data processed. It can be administered in the same moment as the privacy policy, to avoid imposing a further burden on consumers. Moreover, structures already in use to address privacy-related rights can be leveraged both in terms of data access and in managing consumer requests. The channel can be created with a major effort on explainability and may use design support such as Legal-Design. Establishing one communication channel may get the user used to receive communication on actions he/she may autonomously perform to enhance the use of its device and/or its security, allowing upgrades to be perceived sooner and easier as insert in a trustworthy relationship between the man-

[103] Article 29 Data Protection Working Party, Article 29 Working Party Guidelines on transparency under Regulation 2016/679, 2018, 16, available at: ec.europa.eu/newsroom/article29/items/622227.

[104] A. M. McDonald – L. F. Cranor, *The Cost of Reading Privacy Policies*, in *A Journal of Law and Policy for the Information Society*, 4, 2008, 543 ss.; P. G. Inglesant - M. A. Sasse, *The true cost of Unusable Password Policies: Password Use in the wild*, SIGCHI - Conference on Human Factors in Computing Systems, New York, 2010; B. Anderson - A. V., Brock Kirwan - D. Eargle - Seth Howard, *Users aren't (necessarily) lazy: Using NeuroIS to explain habituation to security warnings*, in *International Conference on Information Systems*, 2014.

ufacturer and the consumer. Moreover, these users that have huge benefit from using IoT technologies but also must rely on them more frequent (for example disabled people) more and cleared information on the type of data manufacturer are collecting will be available, hopefully accompanied by efficient mechanisms to change preferences and settings.



Data-Oriented Strategies:

1) *Minimize:* The amount of processed personal data should be restricted to the minimal amount possible.
2) *Hide:* Any personal data, and their interrelationships, should be hidden from plain view.
3) *Separate:* Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4) *Aggregate:* Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.

Process-Oriented Strategies:

1) *Inform:* Data subjects should be adequately informed whenever personal data is processed.
2) *Control:* Data subjects should be provided agency over the processing of their personal data.
3) *Enforce:* A privacy policy compatible with legal requirements should be in place and should be enforced.
4) *Demonstrate:* Be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

Figure 2. Privacy and Design strategies of J.-H. Hoepman, Source: C. Li and B. Palanisamy, Privacy in Internet of Things: From Principles to Technologies," in *IEEE Internet of Things Journal*

This type of solution can itself be structured in a segmented manner, exploiting principles of "privacy by design". Among the strategies that may better match the analysis produced so far, one wants to be highlighted. A strategy proposed by Hoepman[105] and taken up by Li and Palanisamy [106] in their paper, consisting of eight "data-oriented" and four "process-oriented" strategies, as better illustrated in Figure 2 below.[107] The presence of process-oriented strategies fit well into business contexts and design strategies have been proved to improve the perception of consumer and the understandability of information given to them.[108]

Finally, this structure is built to respect the very nature of Internet of Things as «several existing IoT systems are designed using a layered architecture. In an IoT system, data is usually collected by end devices, transmitted through communication networks, processed by local/remote servers and finally provided to various applications. Thus, […] data as it flows through multiple layers of the architecture stack, needs […] protection at all layers. Here, implementing proper [data] design strategies based on the roles of the layers in the lifecycle of the data is important. Otherwise, techniques implemented at a specific layer may become either insufficient ([for example legal requirements are] breached at other layers) or redundant ([data] has been protected by techniques implemented at other layers)».[109] The said approach can also be a starting point for manufacturers that can work in a compliant environment from the very first moment

[105] J. H. Hoepman, *Privacy Design Strategies*, in *Information and Communication Technology*, in N. Cuppens-Boulahia – F. Cuppens – S. Jajodia – A. Abou El Kalam – T. Sans (eds.), *ICT Systems Security and Privacy Protection*, SEC 2014. IFIP Advances in Information and Communication Technology, vol 428, Berlin - Heidelberg, 2014, 446 ss.

[106] C. Li – B. Palanisamy, *Privacy in Internet of Things: From Principles to Technologies*, in *IEEE Internet of Things Journal,* 2019, 488 ss.

[107] A graphic summary of the strategies highlighted by Hoepman can be found in the work of C. Li and B. Palanisamy, *Privacy in Internet of Things: From Principles to Technologies*, in *IEEE Internet of Things Journal*, 2019, 488 ss.

[108] Many studies were conducted on the topic by Professor Cranor, among others: L. F. Cranor, *Necessary but not sufficient: standardized mechanisms for privacy notice and choice*, in *Journal on Telecoomunication & High Technology Law,* 10, 2012, 273 ss.

[109] C. Li - B. Palanisamy, *Privacy in Internet of Things: From Principles to Technologies,* cit.

a new technology is thought and created. This can even enhance the interoperability among smart devices, facilitating even more conversations with consumers and save time and energy.[110]

The purpose of this work was to highlight how IoT asks for a multidisciplinary approach[111] to be regulated. Internet of Things and its implications with the life of consumers must be looked at from a legislative point of view, but to better govern its implications business strategies (meaning with it communication plans, economical tactics and process considerations) must also be considered and this will mainly show in the relationships with final costumers. Efforts from different areas and sectors are required and end-users shall not only be involved but products and services must be designed as user-centric. To reach such level of involvement context shall be dynamic and integrated, «given the pervasive, distributed and dynamic nature of IoT»[112] where high-level information is provided to consumers in a trustworthy form and in a transparent environment. This can result in scenarios where platforms are studied in a user-centric way and where accessibility and accountability become a recognisable distinctive element, capable of becoming a reputational benefit for business and entities.

[110] A. Saeed et al., *Energy Efficient Hybrid IoT System for Ambient Living,* Switzerland, 2022.

[111] A. Skarmeta et al., *User-Centric Privacy*, in S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Cham, 2019, 9 ss.

[112] Ivi, 200.